program

OUR ADDRESS:

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

2600

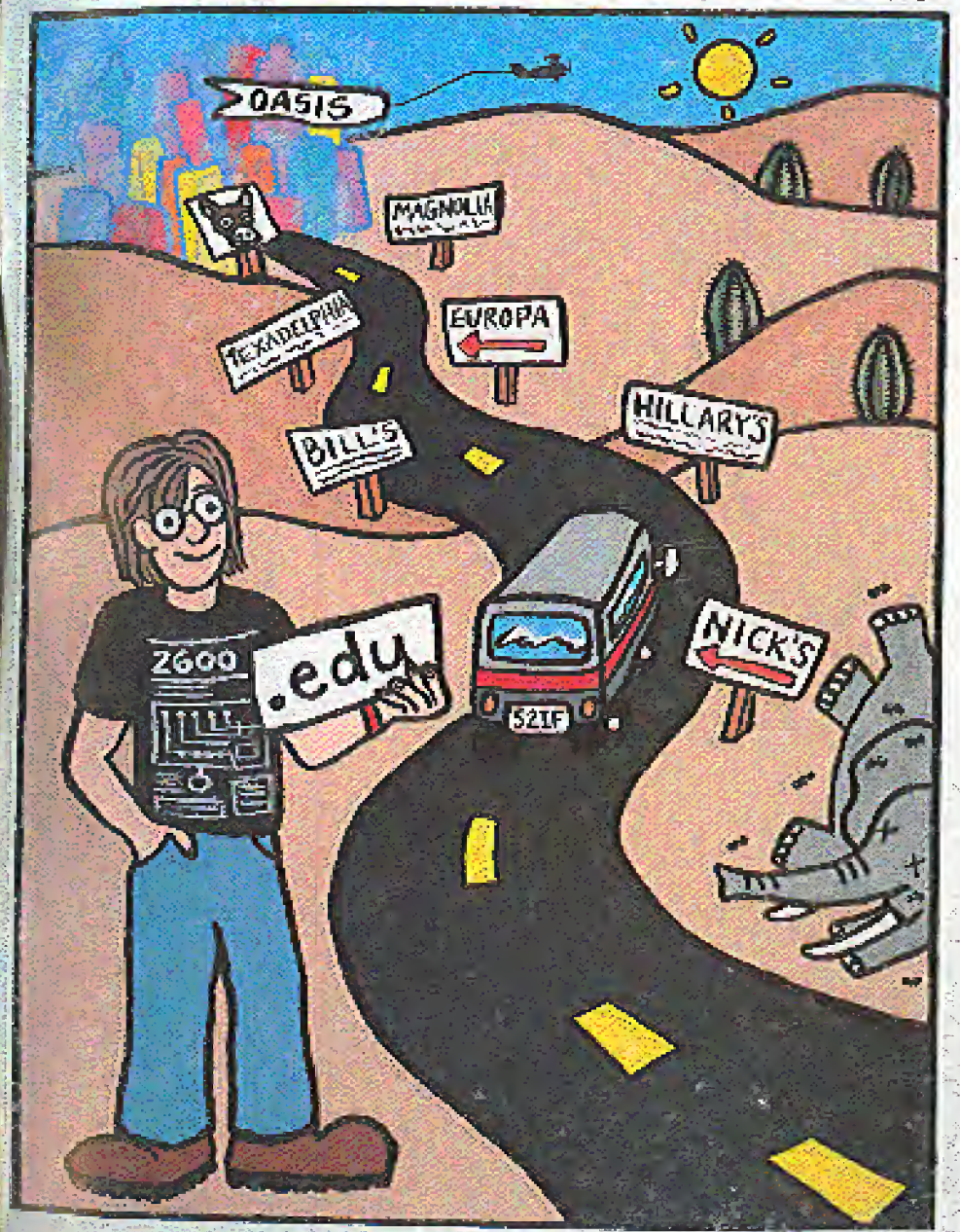
The Hacker Quarterly

VOLUME TEN, NUMBER ONE

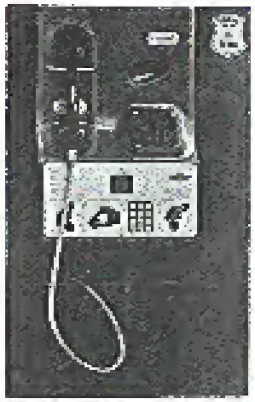
SPRING 1993

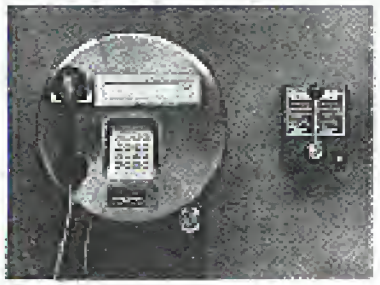
$4

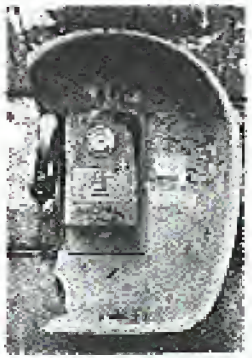
TEXAS FEDEX NOFIVE:



EUROPEAN PAYPHONES







LEFT TO RIGHT FROM THE TOP: Budapest, Hungary; Salzburg, Austria; Munich, Germany (with emergency call handle - left for fire, right for police); Sofia, Bulgaria ("Out of Order" written above dialer); Sofia, Bulgaria ("Out of Order" strongly implied). ***PHOTOS BY KISHON***

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. REWARD FOR MONGOLIAN PAYPHONES!

2600 (ISSN 0749-3851) *is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: *2600@well.sf.ca.us*

2600 **Office Line: 516-751-2600,** *2600* **FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tamprut

Artwork
Affra Gibbs

"The Secret Service didn't do a good job in this case. We know no investigation took place. Nobody ever gave concern as to whether statutes were involved. We know there was damage." - Judge Sparks, Steve Jackson vs. Secret Service, January 28, 1993

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the digital majority.
Technical Expertise: Rop Gonggrip, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Jon L., Steve J., Franklin, Ozona and the Austinites.

Cellular Magic

by Bioclog

Let me start out by saying this article won't be in the best of technical content as I'll be skipping around a little quoting data from various manuals as it pops into my mind. It will however allow anyone that reads it thoroughly and obtains the manuals and equipment described within, to do virtually anything regarding cellular!

ESN: Electronic Serial Number (every cellular has one in Rom)

MIN: The cellular's phone number (this comes in every cellular's Rom)

Reverse Channel: The channel the cellular phone broadcasts on.

Forward Channel: The channel the cell site broadcasts on.

Remember these key terms as they are the crucial essentials.

Most cellulars have the ESN/MIN located in an encovulation located somewhere on the circuit board (older cellulars may not have an ESN.) These are usually 27c256 or 27c512 eproms which can be burned or changed by standard eprom burners. They also reside in the cellular's programming which can be changed.

When you power up a cellular, it sends its ESN/MIN to the cell site on the reverse channel. The cell site then returns the MIN with an OK signal if their database verifies the ESN/MIN. Some newer cell site software will verify the ESN/MIN with the CO. before allowing the call. If everything is OK, the cellular will then be able to place a call.

The reverse channels ESN/MIN and related data can be captured by equipment which we'll list later.

It seems like some wizard(s) have captured other people's ESN/MIN and burned new eproms enabling another cellular phone to use as the originals. Rumor has it that hackers have gone as far as actually changing the eproms' software whereby the program jumps past the ESN/MIN address at the eproms to an address location that can be programmed into memory via the handset! Yet another rumor has it that some even got as far as re-programming the software to capture other cellulars' ESN/MIN and automatically store the data in memory. This naturally allows someone to place fraudulent calls while frequently changing ESN/MINs to avoid all forms of detection. The cell sites usually use frequencies on the two-wire/four A band or forward channels. The reverse channels are usually 45 mhz below the forward channels. These reverse channels are the ones scanned by "telltowers dogs" (who steal others' ESN/MINs for fraudulent use. Note that one hacker seems to think one can use a '220 Uncompiler/Compiler on the eproms' software of some cellulars. (The shame of it all!) Other cellulars use different but common microprocessors of which compilers/decompilers are easily available.

Now that you have the theory behind cellular phreaking, I'll continue on to some background and technical info.

Cellular Overview

A cell system divides the service area into small, low power areas called cells. A cell system has a continuous pattern of these cells, each having a 1 to 40 mile radius (usually 2-10 miles). Within each cell is a base station which contains several transceivers and control equipment for the channels assigned to that cell. These are all connected to an MTSO which is in turn connected to a CO (Central Office) switch. Each cell operates on its assigned channel and may have numerous paging and voice channels assigned to it.

The cellular radio frequencies have been divided by the FCC into two equal bands to allow two different systems to coexist and compete in the same area. Originally there were 666 channels, but that was expanded to 832 in 1988, and with NAMPS to 2412 in 1991.

Band A
Non Wireline
Voice channels: 021-312
Control channels: 313-333
(395 AMPS/1leg NAMPS)

Band B
Wireline
Voice channels: 355-686
Control channels: 334 354
(395 AMPS/1leg NAMPS)

Control channels are used to send and receive only digital data between the cellular phone and the cell base station. The 21 control channels in each band may be dedicated to two different applications: access and paging channels.

The data on the forward control channels provides such info as the system identification number and range of channels to scan to find the strongest paging channels. Access channels are used to respond to a page or to originate a call. The system and the cell phone will use access channels where 2-way data handshaking occurs to determine the initial voice channel. Paging channels, if used, are the holding place for an idle cell phone. When the call is received at the central controller for a cellular phone, the paging signalling will start on a paging channel. In many systems, both control channel functions will be served by the same access channel for a particular cell. Multiple paging channels are only used in high density areas.

NAM: Number assignment Module. This is a memory component (usually an eprom/eeprom) that contains a cell phone's ESN/MIN/SCM, lock code, etc. Some phones can be re-programmed via the handset so one can change their MIN several times (usually the phone's software locks it up after three to 20 MIN changes). This feature was used to deceive cell sites when roaming. Newer cell site software is quickly making this trick obsolete (the problem being that one cannot change the ESN via NAM function programming unless one reverses the system software).

One must know, there is no distributed intelligence in the first generation of cellular systems. At these cellular base stations there is little or no monitoring equipment of any kind.

There are a mix of 3 watt, 1.2 watt, and 600 milliwatt cellular phones in use today. (Keep this in mind as the power of a cellular phone is stored in ROM and transmitted along with the ESN/MIN and the coding must be correct.) 3 watt = mobiles, 1.6 watt = transportables, 600 milliwatt = portables.

IS-41: The newest standard that will let cell switches from different vendors hand-off and deliver calls and transfer subscriber data profiles (newest version is Revision B). This document contains tons of useful info and can be found at public libraries, etc. IS-41 rev B is published by AT&T, although the original rev 0 published in 1987 or rev A published in 1990 may come in handy when dealing with older/smaller MTSO's (Mobile Telephone Switching Offices) that haven't upgraded yet.

MTSO's typically use fiber optic links to cell sites or an 18 ghz microwave link. A cell site in turn can probably use a 38 ghz microwave link to a microcell transmitter. TDMA and CDMA are both vying to become the industry standard.

SST: As soon as a user turns on a cell phone the MIN/ESN for that phone will be carried as an SS7 network message to a database, known as the home location register (HLR) within the user's home carrier system. The HLR will provide information for validation as well as customer profile info for advanced features such as voice mail. That info will then be be relayed to a second database, the visitor location register, maintained by the carrier that is hosting the roaming cell. They hope to reduce fraud by checking the ESN with real time validation on a per call basis. The current system is unable to detect fraud until after a caller has made his first call. (This system simply uses a customer's calling profile to detect an unusual calling pattern.) Those changing ESN/MIN's often cannot be detected!

Cell relay uses fixed length packets - 48 bytes for the payload and five bytes for the header. Two existing cell relay standards are IEEE 802.6 (DQDB) and ATM. They differ only in content of the header.

Each cellular has two channels associated with it, the transmit (REVERSE) and the receive (FORWARD).

Reverse freqs: 824-845mhz

Forward freqs: 869-894 mhz

Conventional dispatch: 896-901 mhz and 851-866.75 mhz

Trunked dispatch: 806.75-824 mhz and 851.75-869 mhz

General reserves: 845-851 mhz, 894-902 mhz, and 926-947 mhz

Channel spacing: 30 mhz AMPS or 10 mhz NAMPS

Reverse Channel Info

Voice channels are used primarily for conversation, with signaling used with quick data bursts or tones to handle cell to cell handoffs, output power control of the cellular radio phone, and special control features. Forward data from the cell site and reverse data from the cell phone are sent using frequency shift keying. The data is formatted into groups of words with a distinct binary preamble that allows the receiver to synchronize to the incoming data. With AMPS, various tones are used. With NAMPS, the data and tones have been replaced by sub audible digital equivalents that ride under the audio. (See EIA - 553 for AMPS or Motorola's NAMPS air interface specification for NAMPS.)

Signaling Tone (ST) and Digital ST (DST)

In AMPS, the signaling tone is a 20 khz signal used by the mobile on the REVERSE channel (REVC) to signal activities or to acknowledge commands from the cell site, including handoffs, alert orders, call terminations, and switch-hook operation. Various burst lengths are used on different ST activities. On NAMPS channels ST is replaced by a digital equivalent called Digital ST (DST) which is the complement of the assigned DSAT. The 10 khz signal is sent for 50 milliseconds.

SAT (Supervisory Audio Tone) and DSAT (Digital SAT)

The supervisory audio tone (SAT) is one of three frequencies.

SAT 0: 5970 hz; **SAT 1:** 6000 hz; **SAT 2:** 6030 hz (plus or minus 2 hz on these three frequencies)

These are used in AMPS signaling. On NAMPS channels SAT is replaced by one of seven sub-audible digital equivalents or words called DSAT.

SAT or DSAT is generated by the cell site checked for frequency or accuracy by the cell phone, then retransponded back to the cell site on the REVERSE voice channel (REVC). The cellular telephone uses (D)SAT to verify that it is tuned to the correct channel after a new voice channel assignment. When the CO signals the mobile regarding the new voice channel, it also tells the mobile of the SAT freq of the (D)SAT vector to expect on the new channel. The returned (D)SAT is used at the cell site to verify the presence of the telephone's signal on the designated frequency.

DSAT: +/- 700hz deviation

Data Transmitted at 10 kbits/sec. Used for sending system orders and mobile identification. In cellular the data is transmitted as Frequency Key Shifting, where the carrier is shifted high 8 khz in AMPS (300 hz in NAMPS) to represent a logic high (or 1), and the carrier is shifted low 8 khz in AMPS (300 hz in NAMPS) to represent a logic low (or 0).

Control channels carry data only. Voice channels carry data and voice signals intermittently.

Audio includes all microphone audio and DTMF while in a call (max mum = 12 kHz deviation AMPS, or 5 kHz dev. NAMPS). DSAT uses 8 kHz deviation only, one hour limit. A selection of seven tones (nine for the high tones) is used to indicate the following digital to AMPS signalling, audio and SAT are suspended by SAT.

Placing a call from a Cellular Phone

When first turned on, the cellular scans through the 832CC's and measures the strength of each signal. It will then tune to the strongest and attempt to decode the received control message. From the overhead the phone can determine if it is in its home system and the range of channels to scan for paging and access. If paging channels are used, the phone next scans each paging channel in the specified range and listens to the strongest one. It's on that channel that the phone will continuously receive overhead message info plus paging messages. At this point the phone idles, continuously updating the overhead message info in its memory and monitoring the paging messages for its telephone number.

When the cellular phone user originates the call, the phone reads the access channels to make sure it's tuned to the strongest one. It then transmits at 10 kbits per sec on the control channel to verify the switch of its MIN (mobile identification number (phone number), its ESN, and the number it wants to reach. The switch verifies the incoming data and assigns a voice channel and an SAT (or DSAT for NAMPS) to the telephone. The phone tunes to the assigned voice channel and verifies the presence of the proper forward SAT frequency or DSAT message. If SAT (DSAT) is correct the phone transmits SAT (DSAT) back to the cell site and activates the forward audio. The cell site detects reverse SAT (DSAT) from the cellular and activates reverse audio. At this point the user can hear the other end ring. SAT (DSAT) is sent and received more or less continuously by both the base station and the phone but SAT (DSAT) is not sent during data transmissions and the phone does not transpond SAT continuously during VOX operation. DSAT is suspended during the transmission of DSI. SAT / signalling tones are only used on AMPS voice channels and the signalling tone is only transmitted by the cellular phone.

Note that the number called, the ESN, MIN etc. are transmitted four or five times and it only takes 360 milliseconds for all 30 this data exchange.

Formulae

Call termination: 10 kbs rate burst for 1.4 seconds.

Freq calc for channels 1-799

Reverse = 825mhz + (Ch # X .03 mhz)

Forward = 870mhz + (Ch # X .30 mhz)

Freq calc for channels 991-1023

Reverse = 825mhz - (.03 mhz X (1023-Ch#))

Forward = 870mhz + (.03 mhz X (1023-Ch#))

Duplex spacing = 45 mhz

Station Class Mark (SCM)

SCM	666 or 832 Ch	VOX	Max Power in Watts
00	666	n	3
01	666	n	1.2
02	666	n	.6
03			
04	666	y	3
05	666	y	1.2
06	666	y	.6
07			
08	832	n	3
09	832	n	1.2
10	832	n	.6
11			
12	832	y	3
13	832	y	1.2
14	832	y	.6
15			

If the SCM is not set properly during programming the system it might have adverse effects on the operation of the phone. It may also flag security violation as a "Tumbled Phone". Some cell phones will only use ESN/MIN's that have the same SCM as their own phone but they plan on rumbling.

Cellular Phone Channel Construction

Here is a method of determining which frequencies are used in a cellular system, and which ones are in what cells. If the system uses OMNICELLS, as most do, you can readily find all the channels in a cell if you know just one of them, using tables constructed with the instructions below.

Cellular frequencies are assigned by channel number, and for all channel numbers, in both wireline and non-wireline systems, the formula is:

Transmit Frequency: (channel number x .030 MHz) + 870 MHz

Receive Frequency: (channel number x .030 MHz) + 825 MHz

"Band A" (one of the two blocks) uses channels 1 to 333. To construct a table showing frequency by cells, put channel 333 in the top left corner of a table. The next one to the right of channel 333 is 332, the next is 331, etc., down to channel 313. Enter channel 312 underneath 333, 311 under 332, etc. Each channel across the top row is the first channel in each cell of the system, each channel down from the column from the first channel is the next frequency assigned to that cell. You may have noted that each channel down is 21 channels lower in number. Usually the data channel used is the highest numbered channel in a cell.

"Band B" uses channels 334 to 666. Construct your table in a similar way, with channel 334 in the upper left corner, 335 the next one to the right. The data channel should be the lowest numbered channel in each cell this time.

Cellular Phone Band A
(Channel 1 to Data)

Cell 1

Channel 1 (333) Tx 879.990 Rx 834.990
Channel 2 (312) Tx 879.960 Rx 834.960
Channel 3 (291) Tx 879.930 Rx 834.930
Channel 4 (270) Tx 879.900 Rx 834.900
Channel 5 (249) Tx 879.870 Rx 834.870
Channel 6 (228) Tx 879.840 Rx 834.840
Channel 7 (207) Tx 879.810 Rx 834.810
Channel 8 (186) Tx 879.780 Rx 834.780
Channel 9 (165) Tx 879.750 Rx 834.750
Channel 10 (144) Tx 879.720 Rx 834.720
Channel 11 (123) Tx 879.690 Rx 834.690
Channel 12 (102) Tx 879.660 Rx 834.660
Channel 13 (81) Tx 879.630 Rx 834.630
Channel 14 (60) Tx 879.600 Rx 834.600
Channel 15 (39) Tx 879.570 Rx 834.570
Channel 16 (18) Tx 879.540 Rx 834.540

Cell 2

Channel 1 (332) Tx 879.990 Rx 834.990
Channel 2 (311) Tx 879.960 Rx 834.960
Channel 3 (290) Tx 879.930 Rx 834.930
Channel 4 (269) Tx 879.900 Rx 834.900
Channel 5 (248) Tx 879.870 Rx 834.870
Channel 6 (227) Tx 879.840 Rx 834.840
Channel 7 (206) Tx 879.810 Rx 834.810
Channel 8 (185) Tx 879.780 Rx 834.780
Channel 9 (164) Tx 879.750 Rx 834.750
Channel 10 (143) Tx 879.720 Rx 834.720
Channel 11 (122) Tx 879.690 Rx 834.690
Channel 12 (101) Tx 879.660 Rx 834.660
Channel 13 (80) Tx 879.630 Rx 834.630
Channel 14 (59) Tx 879.600 Rx 834.600
Channel 15 (38) Tx 879.570 Rx 834.570
Channel 16 (17) Tx 879.540 Rx 834.540

Cell 3

Channel 1 (331) Tx 879.990 Rx 834.990
Channel 2 (310) Tx 879.960 Rx 834.960
Channel 3 (289) Tx 879.930 Rx 834.930
Channel 4 (268) Tx 879.900 Rx 834.900
Channel 5 (247) Tx 879.870 Rx 834.870
Channel 6 (226) Tx 879.840 Rx 834.840
Channel 7 (205) Tx 879.810 Rx 834.810
Channel 8 (184) Tx 879.780 Rx 834.780
Channel 9 (163) Tx 879.750 Rx 834.750
Channel 10 (142) Tx 879.720 Rx 834.720
Channel 11 (121) Tx 879.690 Rx 834.690
Channel 12 (100) Tx 879.660 Rx 834.660
Channel 13 (79) Tx 879.630 Rx 834.630
Channel 14 (58) Tx 879.600 Rx 834.600
Channel 15 (37) Tx 879.570 Rx 834.570
Channel 16 (16) Tx 879.540 Rx 834.540

Cell 4

Channel 1 (330) Tx 879.990 Rx 834.990
Channel 2 (309) Tx 879.960 Rx 834.960
Channel 3 (288) Tx 879.930 Rx 834.930
Channel 4 (267) Tx 879.900 Rx 834.900
Channel 5 (246) Tx 879.870 Rx 834.870
Channel 6 (225) Tx 879.840 Rx 834.840
Channel 7 (204) Tx 879.810 Rx 834.810
Channel 8 (183) Tx 879.780 Rx 834.780
Channel 9 (162) Tx 879.750 Rx 834.750
Channel 10 (141) Tx 879.720 Rx 834.720
Channel 11 (120) Tx 879.690 Rx 834.690
Channel 12 (99) Tx 879.660 Rx 834.660
Channel 13 (78) Tx 879.630 Rx 834.630
Channel 14 (57) Tx 879.600 Rx 834.600
Channel 15 (36) Tx 879.570 Rx 834.570
Channel 16 (15) Tx 879.540 Rx 834.540

Cell 5

Channel 1 (329) Tx 879.990 Rx 834.990
Channel 2 (308) Tx 879.960 Rx 834.960

Channel 3 (287) Tx 879.930 Rx 834.930
Channel 4 (266) Tx 879.900 Rx 834.900
Channel 5 (245) Tx 879.870 Rx 834.870
Channel 6 (224) Tx 879.840 Rx 834.840
Channel 7 (203) Tx 879.810 Rx 834.810
Channel 8 (182) Tx 879.780 Rx 834.780
Channel 9 (161) Tx 879.750 Rx 834.750
Channel 10 (140) Tx 879.720 Rx 834.720
Channel 11 (119) Tx 879.690 Rx 834.690
Channel 12 (98) Tx 879.660 Rx 834.660
Channel 13 (77) Tx 879.630 Rx 834.630
Channel 14 (56) Tx 879.600 Rx 834.600
Channel 15 (35) Tx 879.570 Rx 834.570
Channel 16 (14) Tx 879.540 Rx 834.540

Cell 6

Channel 1 (328) Tx 879.990 Rx 834.990
Channel 2 (307) Tx 879.960 Rx 834.960
Channel 3 (286) Tx 879.930 Rx 834.930
Channel 4 (265) Tx 879.900 Rx 834.900
Channel 5 (244) Tx 879.870 Rx 834.870
Channel 6 (223) Tx 879.840 Rx 834.840
Channel 7 (202) Tx 879.810 Rx 834.810
Channel 8 (181) Tx 879.780 Rx 834.780
Channel 9 (160) Tx 879.750 Rx 834.750
Channel 10 (139) Tx 879.720 Rx 834.720
Channel 11 (118) Tx 879.690 Rx 834.690
Channel 12 (97) Tx 879.660 Rx 834.660
Channel 13 (76) Tx 879.630 Rx 834.630
Channel 14 (55) Tx 879.600 Rx 834.600
Channel 15 (34) Tx 879.570 Rx 834.570
Channel 16 (13) Tx 879.540 Rx 834.540

Cell 7

Channel 1 (327) Tx 879.990 Rx 834.990
Channel 2 (306) Tx 879.960 Rx 834.960
Channel 3 (285) Tx 879.930 Rx 834.930
Channel 4 (264) Tx 879.900 Rx 834.900
Channel 5 (243) Tx 879.870 Rx 834.870
Channel 6 (222) Tx 879.840 Rx 834.840
Channel 7 (201) Tx 879.810 Rx 834.810
Channel 8 (180) Tx 879.780 Rx 834.780
Channel 9 (159) Tx 879.750 Rx 834.750
Channel 10 (138) Tx 879.720 Rx 834.720
Channel 11 (117) Tx 879.690 Rx 834.690
Channel 12 (96) Tx 879.660 Rx 834.660
Channel 13 (75) Tx 879.630 Rx 834.630
Channel 14 (54) Tx 879.600 Rx 834.600
Channel 15 (33) Tx 879.570 Rx 834.570
Channel 16 (12) Tx 879.540 Rx 834.540

Cell 8

Channel 1 (326) Tx 879.990 Rx 834.990
Channel 2 (305) Tx 879.960 Rx 834.960
Channel 3 (284) Tx 879.930 Rx 834.930
Channel 4 (263) Tx 879.900 Rx 834.900
Channel 5 (242) Tx 879.870 Rx 834.870
Channel 6 (221) Tx 879.840 Rx 834.840
Channel 7 (200) Tx 879.810 Rx 834.810
Channel 8 (179) Tx 879.780 Rx 834.780
Channel 9 (158) Tx 879.750 Rx 834.750
Channel 10 (137) Tx 879.720 Rx 834.720
Channel 11 (116) Tx 879.690 Rx 834.690
Channel 12 (95) Tx 879.660 Rx 834.660
Channel 13 (74) Tx 879.630 Rx 834.630
Channel 14 (53) Tx 879.600 Rx 834.600
Channel 15 (32) Tx 879.570 Rx 834.570
Channel 16 (11) Tx 879.540 Rx 834.540

Cell 9

Channel 1 (325) Tx 879.990 Rx 834.990
Channel 2 (304) Tx 879.960 Rx 834.960
Channel 3 (283) Tx 879.930 Rx 834.930
Channel 4 (262) Tx 879.900 Rx 834.900
Channel 5 (241) Tx 879.870 Rx 834.870
Channel 6 (220) Tx 879.840 Rx 834.840
Channel 7 (199) Tx 879.810 Rx 834.810
Channel 8 (178) Tx 879.780 Rx 834.780
Channel 9 (157) Tx 879.750 Rx 834.750
Channel 10 (136) Tx 879.720 Rx 834.720
Channel 11 (115) Tx 879.690 Rx 834.690
Channel 12 (94) Tx 879.660 Rx 834.660
Channel 13 (73) Tx 879.630 Rx 834.630
Channel 14 (52) Tx 879.600 Rx 834.600
Channel 15 (31) Tx 879.570 Rx 834.570
Channel 16 (10) Tx 879.540 Rx 834.540

Cell 10

Channel 1 (324) Tx 879.990 Rx 834.990
Channel 2 (303) Tx 879.960 Rx 834.960
Channel 3 (282) Tx 879.930 Rx 834.930
Channel 4 (261) Tx 879.900 Rx 834.900
Channel 5 (240) Tx 879.870 Rx 834.870
Channel 6 (219) Tx 879.840 Rx 834.840
Channel 7 (198) Tx 879.810 Rx 834.810
Channel 8 (177) Tx 879.780 Rx 834.780
Channel 9 (156) Tx 879.750 Rx 834.750
Channel 10 (135) Tx 879.720 Rx 834.720
Channel 11 (114) Tx 879.690 Rx 834.690
Channel 12 (93) Tx 879.660 Rx 834.660
Channel 13 (72) Tx 879.630 Rx 834.630
Channel 14 (51) Tx 879.600 Rx 834.600
Channel 15 (30) Tx 879.570 Rx 834.570
Channel 16 (9) Tx 879.540 Rx 834.540

Cell 11

Channel 1 (323) Tx 879.990 Rx 834.990
Channel 2 (302) Tx 879.960 Rx 834.960
Channel 3 (281) Tx 879.930 Rx 834.930
Channel 4 (260) Tx 879.900 Rx 834.900
Channel 5 (239) Tx 879.870 Rx 834.870
Channel 6 (218) Tx 879.840 Rx 834.840
Channel 7 (197) Tx 879.810 Rx 834.810
Channel 8 (176) Tx 879.780 Rx 834.780
Channel 9 (155) Tx 879.750 Rx 834.750
Channel 10 (134) Tx 879.720 Rx 834.720
Channel 11 (113) Tx 879.690 Rx 834.690
Channel 12 (92) Tx 879.660 Rx 834.660
Channel 13 (71) Tx 879.630 Rx 834.630
Channel 14 (50) Tx 879.600 Rx 834.600
Channel 15 (29) Tx 879.570 Rx 834.570
Channel 16 (8) Tx 879.540 Rx 834.540

Cell 12

Channel 1 (322) Tx 879.990 Rx 834.990
Channel 2 (301) Tx 879.960 Rx 834.960
Channel 3 (280) Tx 879.930 Rx 834.930
Channel 4 (259) Tx 879.900 Rx 834.900
Channel 5 (238) Tx 879.870 Rx 834.870
Channel 6 (217) Tx 879.840 Rx 834.840
Channel 7 (196) Tx 879.810 Rx 834.810
Channel 8 (175) Tx 879.780 Rx 834.780
Channel 9 (154) Tx 879.750 Rx 834.750
Channel 10 (133) Tx 879.720 Rx 834.720
Channel 11 (112) Tx 879.690 Rx 834.690
Channel 12 (91) Tx 879.660 Rx 834.660
Channel 13 (70) Tx 879.630 Rx 834.630
Channel 14 (49) Tx 879.600 Rx 834.600
Channel 15 (28) Tx 879.570 Rx 834.570
Channel 16 (7) Tx 879.540 Rx 834.540

Cell 13

Channel 1 (321) Tx 879.990 Rx 834.990
Channel 2 (300) Tx 879.960 Rx 834.960
Channel 3 (279) Tx 879.930 Rx 834.930
Channel 4 (258) Tx 879.900 Rx 834.900
Channel 5 (237) Tx 879.870 Rx 834.870
Channel 6 (216) Tx 879.840 Rx 834.840
Channel 7 (195) Tx 879.810 Rx 834.810
Channel 8 (174) Tx 879.780 Rx 834.780
Channel 9 (153) Tx 879.750 Rx 834.750
Channel 10 (132) Tx 879.720 Rx 834.720
Channel 11 (111) Tx 879.690 Rx 834.690
Channel 12 (90) Tx 879.660 Rx 834.660
Channel 13 (69) Tx 879.630 Rx 834.630
Channel 14 (48) Tx 879.600 Rx 834.600
Channel 15 (27) Tx 879.570 Rx 834.570
Channel 16 (6) Tx 879.540 Rx 834.540

[illegible]

Cell #24

[illegible]

Cell #25

[illegible]

Cell #[illegible]

[illegible]

Cell #[illegible]

[illegible]

Cell #18

[illegible]

Cell #[illegible]

[illegible]

Cell #20

[illegible]

Cell #21

[illegible]

Cellular Phone Band B
(Channel 1 is Base)

Cell #1

[illegible]

Cell #2

[illegible]

Cell #3

[illegible]

Cell #4

[illegible]

Cell #5

[illegible]

[illegible]

Cell #6

[illegible]

Cell #7

[illegible]

Cell #8

[illegible]

Cell #9

[illegible]

Cell #10

[illegible]

Cell #11

[illegible]

Cell #12

[illegible]

Cell #13

[illegible]

Cell #14

[illegible]

Cell #15

[illegible]

Cell #16

[illegible]

Cell #17

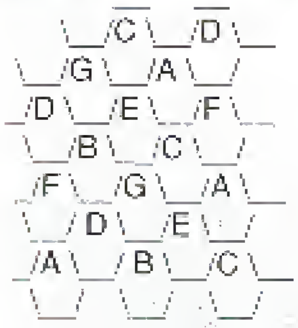
[illegible]

Cell #18

[illegible]

[illegible]	[illegible]	[illegible]
Cell #19	Cell #20	Cell #21
[illegible]	[illegible]	[illegible]

Cellular Phone Frequency and Cell Construction



This represents how a cellular system might be laid out. Cells A and B never share a common border. Neither do B and C, A and G, etc. Cells that are next to each other are never assigned adjacent frequencies. They always differ by at least 60 kiloHertz. To track a mobile phone as it changes cells, do the following. Let's put the mobile in a B cell. When the mobile switches frequencies, you know that he could only go to a D, E, F, or G cell because A and C have adjacent frequencies. The two tables below will help you determine which channel cells can go next to each other. You can contact your local cellular phone company and see if they have any maps of the cells available. This is not a sure thing, but it couldn't hurt to try.

Cells that can go next to each other:

Cell	Compatible cells
A	C, D, E, F
B	D, E, F, G
C	E, F, G, A
D	F, G, A, B
E	G, A, B, C
F	A, B, C, D
G	B, C, D, E

Here is a frequency/cell layout chart. The cell frequencies are used by the cell site towers, and the mobile frequencies are the input frequencies used by the cars.

A	B	C	D	E	F	G

WIRELINE COMPANY CELL FREQUENCIES (BAND B)

Voice Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Digital Control Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

WIRELINE COMPANY MOBILE FREQUENCIES (BAND B)

Voice Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Digital Control Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

NON-WIRELINE COMPANY CELL FREQUENCIES (BAND A)

Digital Control Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Voice Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

NON-WIRELINE COMPANY MOBILE FREQUENCIES (BAND A)

Digital Control Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Voice Channels

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

(continued on page 32)

TROUBLE IN THE WHITE HOUSE

by Charlie Zee

Tuesday, January 26, the White House phone number 456-1414 is busy. In fact, all the White House numbers seem to be busy. And so it's been for the past few days at the White House. There's no way to get through. Is there something wrong with the White House phones? No, said Robert Calhoun, assistant to Delano Lewis, president of C&P Telephone. "We checked on it yesterday. The actual equipment is working fine. There is just a tremendous amount of calls coming into the White House switchboard as well as the Capitol. It appears to me personally that this is something new. That people want to take an interest in their government. They want to speak to the president directly."

Perhaps. But this has been going on for days. Old-timers have never seen anything like it. There were some times during the Watergate stories that the lines would get busy, and the day after Reagan was shot. But hour after hour? Day after day? The White House phone system is designed to handle demands comparable to those of, say, Desert Storm. It has its own dedicated central-office size switching center, said Michael Daley, a spokesman for C&P. The telephone company's normal central offices in Washington usually route traffic for dozens of blocks of office buildings.

As far as who's answering those many lines, the White House won't say. Alex Nagy, director of telephone services (called at the same number he had during the Bush administration), would not even come to the phone. His assistant said: "We do not give out any details."

However, one former White House staffer said there are perhaps a half dozen operators usually working at any one time. He said they "are the top of their profession and career civil servants."

It's definitely not business as usual at the White House according to Joel Garreau of the *Washington Post*. High and low officials throughout town, supplicants and power brokers, can't get through. At a key moment in the recent confirmation hearings for Attorney General-designate Zoe Baird, Senator Joseph Biden got so frustrated trying to get through to the president that he told aides if he didn't hear from Bill Clinton in five minutes, he was going out to the floor to flatly announce his opposition. That broke through the clutter. Somehow Clinton got back to him instantly.

Is it easier for the Russians? With the hot line and all? No, said embassy press counselor Vladimir Derbenev at 347-1347. The White House's direct connection is only to Moscow, not the embassy.

What about the Iraqis? How would they get through to the president? Fire a few rounds at the Kitty Hawk? A hurried call to their embassy at 483-7500... No, we have not been having any particular problem with the White House phones, came the answer. That's because we can't call the White House much. Our problem is with the United Nations.

And bypassing the White House switchboard and trying to reach somebody's direct line is no snap. Call the old number for the press office listed in the *National Journal's Capital Source* directory, and the call is answered by the office of the chief of staff. Ask them if anybody is keeping track of how many incoming calls there have been, and you are directed to the staff secretariat. Ask who is the head of that, and the person at the office of the chief of staff does not know. There's no new White House phone directory out yet even for people inside the building. Track is being kept on the backs of envelopes; some numbers have changed. "We're working on hit-or-miss temporary listings. They're not complete," said one White House source.

On January 26, the telephonic gridlock had sloshed over into the Capitol Hill lines. The office of Senator Dan Coates (R-Ind.), a vocal opponent of Clinton's proposal to rescind the ban on homosexuals serving in the armed forces, numbers about 1,000 by Tuesday night - about 16 to 1 in favor of the ban, the Associated Press reported. The office of one prominent liberal senator said it received 500 to 700 calls, with a majority in favor of allowing homosexuals in the military, said an aide.

And the main Capitol Hill number, 224-3121, has remained busy. Could this all be people wound up in the gay issue? In fact, no, said one White House official when finally reached. "The switchboard is totally swamped, but the calls are running about 50-50," said the source. "Half concern the issue of gays in the military. But the other half is people who are perceiving waffles on campaign pledges. Clinton promised many things. And now people are worried that things are not going to turn out that way. People are more involved with this administration than in the past. Even the [mechanized] comment line has never been like this. Everybody and their brother feels like they can call in, and right now, they are."

Then again, some of those calls are like the ones made to David Watkins. If anybody should know what's going on with the phones, he ought to be the one, seeing as how he's assistant to the president for the office of administration and management. And somebody had him listed at 456-6797.

That, in fact, turns out to be the office of the chief of staff, which could still make sense since that's who he works for, according to the table of organization handed out back in Little Rock. But no. The person who answered the phone at the office of the chief of staff said she did not have him on any of her lists. Nor did she know where he sat or what his phone number might be. In fact, she had never heard of him.

2600 NOW HAS A VOICE BBS THAT OPERATES EVERY NIGHT BEGINNING AT 11:00 PM EASTERN TIME. FOR THOSE OF YOU THAT CAN'T MAKE IT TO THE MEETINGS, THIS IS A GREAT WAY TO STAY IN TOUCH. CALL 0700-751-2600 USING AT&T (IF YOU DON'T HAVE AT&T AS YOUR LONG DISTANCE COMPANY, PRECEDE THE ABOVE NUMBER WITH 10288). THE CALL COSTS 15 CENTS A MINUTE AND IT ALL GOES TO AT&T. YOU CAN ALSO LEAVE MESSAGES FOR 2600 WRITERS AND STAFF PEOPLE AROUND THE CLOCK.

beige box construction

by The Phoenix

Many tasks involving phone line work (such as installing a new extension, etc.) are much easier when you have a lineman's handset. Since a typical tone/pulse switchable model sells for about $300 many people opt to build their own. Such an improvised handset is called a beige box. I will begin this article by repeating the instructions for making one. Next I will mention what the lineman's handset has that the generic box lacks and explain how to add these features.

To construct a basic beige box you need a one piece phone, preferably pulse/tone switchable, a pair of alligator clips (one red and one black for the traditional look), and some tools (wire cutters, wire strippers, long nose pliers, PVC electrical tape, and a soldering iron). If the phone has no line cord you will need that too. Cut the wire about four feet from the phone. Expose and strip the red and green wires. Connect the red alligator clip to the red wire and the black clip to the green wire. For a good connection these should be soldered. Wrap the connections in electrical tape. It's that simple! In the off-hook state this device will behave just like a lineman's handset in the Talk mode.

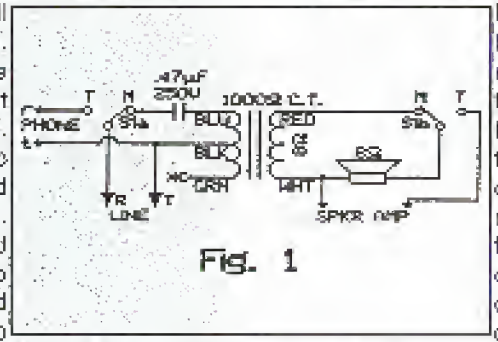


Fig. 1

Lineman's handsets have a Talk/Monitor switch instead of a switchhook. In the Monitor mode it does not merely go on-hook like our beige box; it becomes a *line tap*. You can monitor everything which transpires on the line: an indispensible testing aid! If no phones are off-hook you will hear a background hum. If you pick up an extension you will hear the click and dial tone. It will not interfere with rotary dialing. If an incoming call arrives you hear the ringing signal (a loud purring).

To add this feature to your beige box you will need a .47 microfarad 250 V capacitor (non electrolytic), an audio matching transformer: eight ohms to 1000 ohms (Radio Shack Cat. #273-1380 will be used in the example), a DPDT switch, and some wire. Refer to Figure 1. Open the phone. Locate the point where the line cord enters. The red wire is the "ring" and is labeled "R" in the figure. The green ("tip") is labeled "T". Points "r" and "t" (lower case) are the points where these connect to the phone circuitry. Disconnect the Ring from the phone circuitry and connect it to the center of one pole of the switch. Run a line from one leg to the point where the Ring used to be. Connect the capacitor to the other leg. Solder the other capacitor lead to the transformer's blue lead. Connect the black lead to the tip. Ignore the green transformer lead (cut it off if it annoys you). The high impedance side is complete.

Now the eight ohm side: Find the earphone leads. (If the colors give any clue as to polarity put the switch on the positive one.) Connect the white wire from the transformer to one of the speaker wires. Disconnect the other speaker wire from the main circuitry and solder it to the center of the free pole on the switch. Attach the red transformer lead to the leg on this pole which corresponds to the capacitor's position on the other pole, i.e. the Monitor position. The remaining switch terminal should be connected to the point from which the speaker wire was removed. With this modification the switchhook becomes somewhat pointless. The ringer can also be removed to make room for the transformer. Test the switch, mount it, and label T and M.

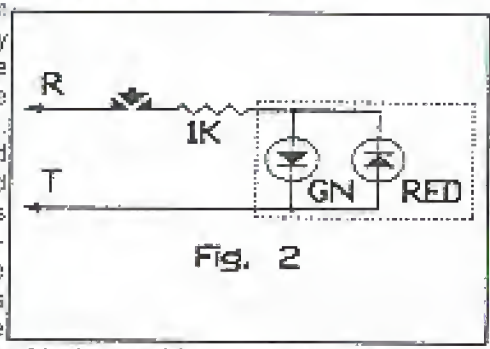


Fig. 2

Many exciting new handsets of the tone/pulse switchable type have an extra switch: KEYPAD: IN/OUT. I assume this is to prevent accidentally dialing with your shoulder. This will not be discussed.

One last feature these new handsets have is a polarity test. This can be useful. Obtain one green and one red LED, an SPST momentary pushbutton, and a 1k ohm resistor. Refer to Figure 2. Connect the anode of the green LED to the cathode of the red one and to the resistor. Tie the cathode of the green to the anode of the red and connect that to the Tip. Connect the free end of the resistor to the button and the other side of the button to the Ring. Make sure that the cathode of the green is wired to the black alligator clip. When the button is pressed the green LED will light if the red clip is on the positive (+) and the black clip on the negative (-). Note: The polarity test will create an off-hook status.

Thanks go to The Exterminator and The Terminal Man for their text file, *Beige Box: Construction and Use* dated Friday 17 May 1985, which detailed the construction reiterated in paragraph two. The type of phone tap I employed in adding the monitor mode was first brought to my attention in a text file by The Phantom (title/date unavailable). Note that if your speaker is not eight ohm you will have to use a different transformer; check with the outfit you get your .47 microfarad capacitor from.

Lastly, Radio Shack no longer carries .47 microfarad capacitors. I wonder why? Other electronics distributors do. You may also find them in phone equipment isolating the ringer from the line.

DESCRAMBLING CABLE

by Dr. Clayton Phorester

If you were thinking about opening your cable box, don't! Most cable boxes have a small metal connector in the front right of the box. Once the lid is off, the connection is broken and a little battery inside remembers. I learned this the hard way with a Pioneer converter. Once the connection breaks, the little channel display on the box will go all screwy, and the only button that will work is the power button. If you *did* open the box, you would now notice that whenever you turn the TV on, it goes to a preset station and can't be changed. This station is usually the one that your box displays when you tune to a premium channel that you don't subscribe to. At any rate, cable companies will fine you around $25 to reactivate your box. And if they think you've tampered with it, that goes up to $1000 (according to California law). All the cable company has to do is press a few keys on their cheap computers in their cozy little offices to get the box at your house back on line. (And you thought their regular rates were bad!)

If you did open it, maybe you could tell them that it fell on the floor during an earthquake or something. Or, you could do what I did. I told my cable operator that I was throwing away a TV, and was going to return my cable box. Well, I returned the box (after I closed it back up, of course) and about a month later I told my cable company that I got a new TV. I went to the cable office and picked up a new box. Result: I got a perfectly good box, while some dumb Wilson got the old tampered- with one! And, of course, the Wilson won't know what the hell's going on when his box doesn't work, so he'll call the cable company and complain. The cable company (arrogant as they all are) will naturally assume that this person was trying to tamper with it, and they aren't gonna believe anything this guy is gonna tell them. *Ha! Ha! Ha!* (That's just my sick sense of humor.)

The point is: *don't open the damn box!* Inside there are a hundred little dials, screws, and thingamabobers, but messing with them won't do you a hell of a lot of good if the box won't respond to any commands in the first place!

I just recently downloaded from a local BBS the following instructions to make a cable descrambler. It appears to have been uploaded in 1988 (how's that for sysop incompetence?) but it's worth a shot anyway. I'm almost certain that it won't work with a handful of cable systems because every one is different in its own little perverse kind of way. In Step 6, the author assumes that you will be using a cable box. I don't think that having a box is a requirement, because I don't have one, and my descrambler works just fine. On my cable system, boxes are an option for old TV's that don't go any higher than Channel 13, and TV's that you want to receive premium channels. So if you have one or not, don't sweat it.

Enough talk! Whip out your wallet, your car keys, your soldering iron, and kick some cable company butt!

How To Build a Pay TV Descrambler

Author Unknown

Materials Required

1 Radio Shack mini-box (RS #270-235)
1 1/4 watt resistor, 2.2k-2.4k ohm (RS #271-1325)
1 75pf-100pf variable capacitor (hard to find)
2 F61a chassis-type coaxial connectors (RS #278-212)
12" No. 12 solid copper wire
12" RG59 coaxial cable

Instructions

1. Bare a length of No. 12 gauge solid copper wire and twist around a 3/8 inch nail or rod to form a coil of nine turns. Elongate coil to a length of 1 1/2 inches and form right angle bends on each end.

2. Solder the variable capacitor to the coil. It doesn't matter where you solder it; it still does the same job. The best place for it is in the center with the adjustment screw facing upward. Note: When it comes time to place coil in box, the coil must be grounded. This can be done by crazy-gluing a piece of rubber to the bottom of the box and securing the coil to it.

3. Tap coil at points 2 1/2 turns from ends of coil and solder to coaxial chassis connectors, bringing tap leads through holes in chassis box. Use as little wire as possible.

4. Solder resistor to center of coil and ground other end of resistor to chassis box, using solder lug and small screw.

5. Drill a 1/2 inch diameter hole in mini-box cover to permit adjustment of the variable capacitor from the outside.

6. Place device in line with existing cable on either side of the converter box and connect to a television set with the piece of RG59 coaxial cable. Set television to HBO channel.

7. Using a plastic screwdriver (or anything else non-metallic), adjust the variable capacitor until picture tunes in. Sit back, relax, and enjoy!

SJG TRIAL: DAY BY DAY:

Secret Service on Trial

BY PACK RANGER NETRUNNER

Day One

DATELINE: January 26, 1993 - the beginning of three strange days of Federal District Court in Austin, Texas. A rare frost lays on the ground and chill air descends on the "birthplace of cyberpunk" as I trek down to Judge Sparks' courtroom. I have to thank my stars at the X-ray desk - politely. Even then some big Federal Marshall goon pulls me out of a puzzled crowd to demand ID and lecture about "weapons in a courtroom". 'Tis a task performed with apprehension because today of all days, the Feds must take the stand - prison for a hill, as improbable as it may seem, at the hand of a mob of Freaks, "Computer Freaks." You can see it written in the eyes of each SS agent surrounding the court room. Today the Feds themselves are on trial; today they can no longer run and hide.

First we must wait for Judge Sparks to clear the docket. A jury deliberates its eventual "guilty" verdict on a guy who'd sent an 11-year-old in to conduct a bank heist, and Sparks prepares to send that guy on his third trip to camp. Outside the parties in our case pace fervently... Ed Cavazos, vice president of EFF-Austin, recent UT/Austin Law School grad and a good friend, lounges off the walls in anticipation. This is Ed's first full case; he's been a sysop for years, runs a popular BBS in Austin called "Bamboo Gardens", and grabbed a lucky break by educating the local newspaper's night-tech law firm - George, Donaldson, and Ford - about the arcane ways of computing and BBS's. Shari Steele of the Electronic Frontier Foundation - major underwriter for the plaintiff's legal fees - works the field for her home office. Joe Abernathy of the *Austin Chronicle* and *Village Voice* - probably the first major newspaper columnist to cover computer underground issues on a regular basis - passes Feds in

Foley

an attempt to uncover dirt. Steve Jackson stands nervously, chatting, trying to maintain a good humor among plaintiff groupies which even includes his room. A vague array of Fed spooks and lawyers crowd the courthouse shadows, avoiding all contact. Lawyers from both sides huddle and haggle in a last minute settlement procedure which dies when the SS claims they "lack enough budget" to cover Steve Jackson Games' legal fees. Well, we'll see, eh?

Sparks delays the trial until after lunch. I overhear SS agents' talk about restaurants, so I tail them and sit down at the next table *after* they enter. They get up in disgust and move to the back of the restaurant.

"The Court calls the case of SJG et al. versus SS et al. to order..." Plaintiff, with lawyer Pete Kennedy at the helm, introduces witnesses: Steffan O'Sullivan, Elizabeth McCoy, and Walter Milliken - SJG writers and users of the seized *Illuminati BBS* who'd joined in the lawsuit as plaintiffs - along with Wayne Bell, developer of WWIV bulletin board software. Government defense introduces Larry Coutorie - famed UT Austin "computer cop" - and SS agents Tim Foley and Barbara Golden.

Timothy Michael Foley takes the stand under cross-examination. Loyola University '84 Law School grad, trial lawyer for 2+ years, Feds of the US Secret Service - a great ole boy in any other life. Foley was the SS agent assigned to the "E911 Document" investigation and his sworn affidavit to Fed Magistrate Stephen Capelle early in 1990 lead to a search warrant for the SS raid on SJG. Foley rambles defensively about his computer expertise, brags of being top dog at SS Computer Fraud School, tells how he learned about "Social Engineering" there in mid 89, only months prior to the decision to raid SJG. Foley talks boldly of *Phrack* #24 and the Craig Neidorf case, sloppily explains BITNET to the judge, then mentions the *Phoenix Project* - a "suspected hacker BBS" operated in Austin by "The Mentor" (aka Loyd Blankenship) and "Eric Bloodaxe" (aka Chris Goggans), and thought by the SS in 1990 to contain secret areas for instruction on "computer crime". One of the sysops worked for SJG and therein lies the only grounds for the raid. However, under oath Foley admits that at the time of his affidavit to Capelle, he didn't have any info showing the E911 document ever even reached the *Illuminati BBS* and SJG. Moreover, Foley confesses he knew that "telecom expert Hank Kluepfel (who enters this grim picture later) had never logged into *Illuminati*." When asked about the allegedly threatening SJG project called *GURPS Cyberpunk*, Foley states: "I did not read through the game."

Not terribly incriminating so far, but enough to show that the SS had not made a full disclosure to Magistrate Capelle before obtaining a search warrant. Even so, never assume the Government is sleeping.

Up walks Mark Batten, a tall, slim, boyish-skinned assistant US Attorney. Batten leans competently in fast he spends most of his off hours playing DOS games to

the Macintosh." I got a Mac in college and I've been doing that ever since" he tells me during lunch). Batten takes Foley off the hook by having him testify that the SS didn't seize most Federal records which limit seizure of equipment from publishers.

Next we get Officer Larry Coutorie on the stand. Coutorie has been with the UT Austin police for years but lately seems to be working the computer crime beat. The SS search warrant against SJG claimed that Officer Coutorie had provided "UT Investor information" about Loyd Blankenship and a list of Coutorie's documents. Under oath, Coutorie denies the alleged snooping, since Blankenship was never affiliated with UT Austin nor in the school database. Coutorie claims the document was printed after the SJG raid. Note that Officer Coutorie is technically "on the other side" from SJG, but in depositions he disavowed himself from the Feds. Rumor has it that the Coutorie's lawyer's car sports a nifty EFF bumper sticker. Ladies and gentlemen, this marks a blow to the Feds. But wait, another SS agent - Barbara Golden from the Chicago area - takes the stand. Golden looks timid, indignant, fearful, like a third grade teacher surprised in a fire drill. She answers in filled, nervous clips of "Yes" and "No". Golden - who conducted the SJG raid and computer equipment seizure - admits under oath that she "didn't know much about computers," claimed she "didn't know about search rules for publishers" but counters that Steve Jackson Games Inc. - the renowned publisher of role-playing game books - wasn't a publisher. Plaintiff calls for a videotape of the raid - recorded by the SS - to be entered as evidence. After several abortive attempts (Sparks jokes, "Let the record show that no one could successfully operate the VCR although there were several attempts by various lawyers") the video finally spins its eerie record of the early morning heist on March 1, 1990. Office walls show news about printing schedules and hallway through seamlessly from SJG walks in ashen, shouting, "We are a publisher!" Ignorance doesn't get much more blatant than this, and rumor has it that cyberpunk science-journalist Bruce Sterling will show a copy of the tape as a backdrop during his next lecture tour.

Steven Guy Jackson jumps into the hot seat next. Steve, who attended law school before becoming a gaming industry entrepreneur in 1980, understands the essence of this game and it shows. Over the course of the afternoon and the next morning, Steve's lawyers guide him through an extended testimony: the nature of role playing games (RPG)... creation of his *GURPS* system for role playing... origins of "cyberpunk" as a literary genre in novels such as *1984* and *Neuromancer*... intentions for the seized *GURPS Cyberpunk* to have been a literary survey. "That book was key to our company's financial well being - distributes judge you on the basis of new product each month." Jackson goes on to describe the *Illuminati BBS*, how he didn't even know *why* it was seized by the Feds and therefore feared replacing it. "We had hard to find out [why the BBS was seized]..." At one point near tears, Jackson explains what appears to be his main conviction against the government: "After the raid, I saw my employees being upset... We couldn't see any way to stay in business without drastic cuts, so we laid off eight people out of 18 ... If the Secret Service had just come with a subpoena we would have

Golden

cleaned or copied every file in the building for them."

Steve closes the first day's testimony with an appalling account of trying to obtain copies of his seized disks - vital business records and publication drafts which were held for months with no explanation - from Agent Foley.

Foley (referring to GURPS Cyberpunk): "Do you realize you're publishing information on how to commit computer crime?"

Jackson: "This is a game."

Foley: "No, this is real."

Day Two

Defense counsel Mark Batten cross-examines Jackson in a cowardly attempt to imply that SJG was in financial trouble before the raid but recovered to profitability afterward. Judge Sparks interrupts: "Because it was raided by the Secret Service? Is the Government claiming they *helped* his business by seizing equipment?"

Games counters with a concerned right hook: "No, your Honor..." - then launches into a special role player how the SJG game *Hacker* resulted from the raid, and how SJG capitalized on publicity surrounding the SS action. Defense tries to pin the issue on Steve.

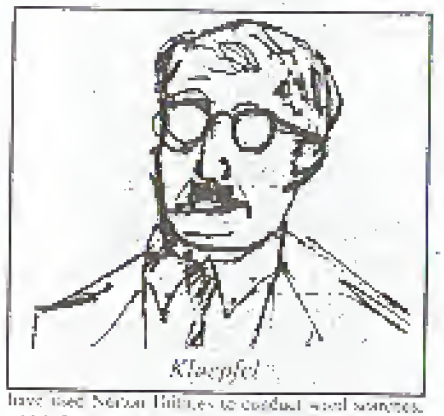
Batten: "Why not just redesign Hacker?"

Jackson: "I'm not crazy. I am a writer, role is the way I tell a story."

Elizabeth McCoy takes the stand next. As an interactive fiction writer for SJG, she'd been a board moderator on part of the seized *Illuminati BBS*. Elizabeth testifies that her project "was seriously damaged by the raid" and goes on to read a private email message that was on the seized BBS and ostensibly "investigated" by the SS. The message contains a beautifully sweary personal letter from SJG

writer Steffan O'Sullivan about another writer at SJG - Walter Milliken - whom she since has married. Milliken takes the stand and also describes the use of email on *Illuminati BBS* for SJG work. Walter understands email quite well, he's a computer scientist for BBN, the firm which created Internet.

Government faces a few cool points here, but Baron tries to resurrect by reading a sworn deposition from SS computer security specialist Larry Boothby who analyzed the seized equipment. Boothby claims to



Kluepfel

have used Norton Utilities to conduct word searches, which Baron explains to Judge Sparks: "He'd type in the word 'hack' and it would show on the screen with surrounding text." Note that Boothby wasn't available since he had resigned from the SS just as the case was scheduled to go to trial "and could not be recalled." Some think Boothby may have taken a fall for the organization. ... As a spoff, his deposition did include unfavorable remarks about Agent Foley's alleged computer expertise: "They might as well have had Mickey Mouse in there."

Next on the dance card, Wayne Bell steps up as an expert witness for SJG. As author of the WWIV software for BBS - which *Illuminati* runs - Wayne's wares run on over 2000 systems, for an audience of 3 million. Wayne had been called in to review the *Illuminati BBS* as soon as the SS had returned it. "It appeared that all the mail had been deleted by March 20, 1990." Wayne testifies that he checked the PC's system clock and verified file time-stamps with phone records which users had provided. "Off by about 6 minutes at most."

Judge Sparks asks to have the term "spoof" defined at several points - burn that into your memory. He claims utter ignorance of computing technology, which plays well into plaintiff's hand. SJG is trying to sue the US Government for damages based on Federal statutes and constitutional law, but the Government is putting a classical defense tactic by snowing the judge with technical terms. So SJG needs to make this as simple and clear-cut as possible.

Next up to the stand comes Henry Michael Kluepfel, alleged computer crime expert and anti-hacker from Bellcore, looking surprisingly like a cross between Woody Allen and Adolf Hitler - whiny, wimpy, and vile. "I provide information related to threats" is the introduction Kluepfel uses to justify his place in life. He goes on to describe how in 1989/90 he'd been investigating the E911 document's spread by logging into suspected BBS under the handle "REUBEN" and looking for files about computer intrusion. He whines at length about *Phrack, Inform*, E911, etc., but admits that (1) the *Phrack* issue in question with the E911 document *didn't* provide any steps for how to break into computers and (2) the information is available to the public anyway - "But not quite what was in the Bellcore document." Judge Sparks becomes visibly lost in Kluepfel's use of technical terms, and shares the pain that Kluepfel just ate his own straw. So Kluepfel continues.... He talks about exploring *Phoenix Project*, about finding a file related to E911, downloading it, providing an affidavit to Bellsouth, then forwarding the file to the US Attorney in Chicago - William Cook.

Early in 1990, the *Phoenix Project BBS* shut down. Kluepfel explains that "Newbin was wondering where *Phoenix Project BBS* might reside since it wouldn't answer. Could Steve Jackson Games' *Illuminati BBS* be the new *Phoenix Project*?" Kluepfel goes on to admit the fatal flaw: "I did not tell Newbin that there was anything connecting Steve Jackson Games other than that Mentor was co-sysop of both BBS's and the both BBS's ran WWIV software."

Again, the judge is enraged in technobabble, and at this point the defense takes up questioning and prompts Kluepfel - the US Government's computer expert - to help educate the judge. Kluepfel testifies about having found evidence on the *Phoenix Project BBS*, including, "Kermit and XModem, which can be used as tools for computer crime." Sparks then speculates about the need for a raid, whether other alternatives were open: "Would it have been possible for the Government to take this issue to another Reebok [sic, should be RSIC] for information?" Kluepfel counters with his own reputation. "I was asked as an expert with 25 years in computer security, network security" - so essentially his word was good enough for the Government to act. So they did.

Hey, this guy is pure weaseliness distilled into a puny frame. During court recess I go outside to track him down, shaking his hand just to experience a pure, raw state of disgust. We chat a bit, talk of our respective tenures at Bell Labs, how he works in a town where I used to live - Red Bank, NJ. Not a bad guy really, a bit nervous and defensive, probably a reasonable response for a person who has just lied under oath to a Federal judge and seems at least intelligent enough to know it.

Now the fireworks begin. Former US Attorney William Cook - who quit rather suddenly after the SJG case reached national news - climbs into the pilot seat. Finally those of us in the SJG peanut gallery recognize who this asshole is, since he'd asked us to shut up during court recess "so as not to pollute my testimony." As if it were possible for Cook utters to pollute what can pass between Walter Milliken and Dana Carvey's rendition of George Bush, indignant and condescending to everyone in the courtroom except for the judge. Cook even interrupts court proceedings to correct plaintiff counsel on proper procedure. This guy got burned by the SS right and now he's sworn to settle. Cook responds to cross-examination about his $79,000 figure for the worth of the "stolen" E911 document. Under oath he specifies that $22,000 was for the purchase of an Edsel word processing software package, several more thousand was for computer hardware used to type the declaration, along with salaries for people doing the typing .... When pressed by plaintiff counsel, Cook admits these junk-heap systems were not used up in the process of typing a few pages.

Moving to the point, Cook admits (1) that he knew about the Privacy Protection Act (PPA - which limits government seizure of equipment from publishers) but didn't advise the SS about its implications prior to the SJG raid, and (2) that he understood the relevant wiretap law in the Electronic Communications Privacy Act (ECPA - which MAY limit interception of email) but didn't advise the SS against seizing a BBS that contained unread mail.

Cook then lies to DOD's Computer Emergency Response Team (CERT) which "briefed" Craig Neidorf about *Prophet* and E911: "As a result, agents sought and received a search warrant" against SJG. Cook explains that after the seizure, two files were identified and deleted - an alleged password cracker called "DE ZIP" and some unspecified software believed to have been illegally copied - however he fails to specify which computer held the deleted wares. Keep that in mind too.

Judge Sparks kicks in to question William Cook for a bit, uncovering two startling items: (1) Cook's admission that the US Attorney's office made no attempt to determine the nature of SJG's business prior to the raid, and (2) Cook's claim that he is "aware of an ongoing investigation about criminal charges against Blankenship and/or Goggans."

Next in line, SJG's restaurant steps up to provide expert testimony about the damages incurred by the raid and confiscation of equipment, records, stationery, etc. The accountant cites several key losses: gaming books not being released, delayed shipments because the BBS as a communications interface for the Tim, layoffs of good talent, impact on Steve Jackson's own time for executive writing, and expenses for litigation. She produces balance sheets, cost estimates, revenue projections, etc., but the Judge seems annoyed. Deciding a seven percent interest rate for present discount values (a financial giveaway to the Government), the accountant arrives at a $2.1 million total for damages. Sparks doesn't seem happy and calls it a day....

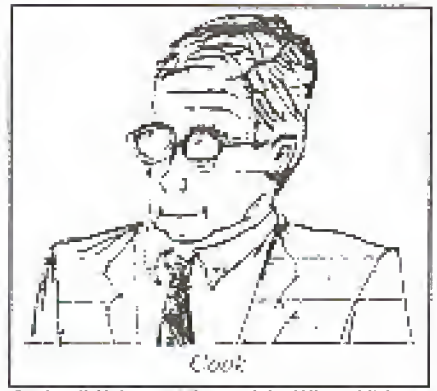
Day Three

After a delay caused by unrelated legal proceedings, Government defense steps up and attempts to have the case thrown out of court, urging Judge Sparks not to risk exceeding the ECPA statute in response. Sparks grows annoyed: "It appears to me that I'd have to rewrite that statute to agree with the Government's case .... It appears that Loyal Blankenship could have prepared to engage in some nasty criminal activity. You see a BBS with a notice about conspiracy. So it would have taken an hour or less to do [the investigation] as it should have been done. Don't you think Congress should decide how far the ECPA should extend? I don't think ECPA applies in any way to this case - so what? Did Blankenship have possession at the time the search warrant was executed or his ability (as sysop) to delete files? I want that answered."

EFF-Austin members drop by to watch the last part of the trial - several students even manage to get out of high school for it - but a Fed Marshall boots them out because the aisles aren't wide enough.

SS Agent Tim Foley steps back up as defense witness. He describes his impression of the confiscated *Illuminati* ("everyone" hates the Government's case about a "potential hacking conspiracy." "It appeared to me to be a fictionalized account of what LOD was doing." Back under cross-examination, he admits there was nothing in the search warrant's affidavit about a threat to national security, the disappearance of the *Phoenix Project BBS*, evidence of the PA story *Project BBS* appearing in SJG, or evidence incriminating any other BBS at SJG.

Foley launches into an account of how Blankenship's former place of work - Nth Graphics in Austin, TX - had also been "visited" at the time of the SJG raid. "We had a record that the E911 document had gone to Nth Graphics. We went there and asked to see the machine but it crashed so we didn't pursue any



Cook

further." Foley testifies a plaintiff's exhibit - a handwritten document by SS agent John Locke which explains that a purported NSA document found at Goggans' home actually was a SJG tape incorrectly

and copyrights on the bottom, i.e. it was just a part of a game.

At this point plaintiff counsel Pete Kennedy and Judge Sparks both question Foley. In a legal equivalent of an online chat, making defense counsel turn pale...

Foley: "It took one week on the machines to analyze the files."

Kennedy: "But the equipment wasn't returned for three months!"

Foley: "Yessir."

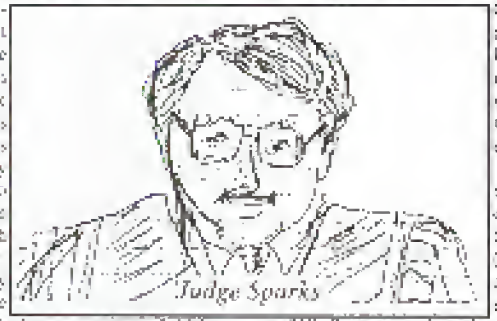
Sparks: "Why?"

Foley: "We had to make reports."

Sparks: "But clearly after one week, the United States of America could have finished analyzing the disks and have returned the equipment to Steve Jackson Games?"

Foley: "I guess."

Foley goes on to say there was never any evidence to incriminate SJG before or after the seizure. Sparks



guesses again, emphatically: "Why couldn't copies of everything be made within seven days and returned to Steve Jackson Games as requested by his lawyer?" So Foley admits there was no reason not to return equipment after March 10, 1990 at the latest. The tragedy is that Foley had been insistent on the raid, and yet he'd only become aware of SJG on February 23, 1990 - just one week prior.

In closing remarks, Judge Sparks reveals a dangerous misconception: "How do I know one illegal material was not in the *GURPS Psychopunk* [sic] dossiers? We know that the computers contained sensitive materials (DST documents) and even illegal materials (DF-ZIP) ... But let's assume a violation with regards to *GURPS Psychopunk* [sic] occurred, what were the damages established by the evidence?" Then he asks both sides to interpret the PPA statute.

Plaintiff specifies the damages to include: loss of BBS and delay of *GURPS Cyberpunk* release, which struck SJG at the worst possible time financially and cost eight people their jobs and reduced SJG's creative talent.

Defense dismisses the damages by claiming that the raid "only delayed *GURPS Cyberpunk* by less than three weeks (a down sized version based on old drafts was released, but), plus better management procedures after the seizure which forced Steve Jackson to spend less time writing and more on business may have been his best business move ever."

Sparks counters this argument: "So the Secret Service is now helping businesses by search and seizure? The officers charged with this 'evil conspiracy' obviously jumped to a conclusion.... Admittedly without evidence they took three computers and 300 disks and ignored Steve Jackson's lawyer's attempts to get back the equipment. It just doesn't pass the smell test for the Government to come in without any evidence against the company and take things that anybody could tell would harm the company. The reason this wasn't done in good faith was lack of investigation by the Secret Service. Evidence shows that by March 2, 1990, somebody in the Government knew a book was involved [in the seizure]. There is no question in my mind that Steve Jackson Games Inc. sustained damages and expenses as a result of misconduct by the US Secret Service ..."

Epilogue

Immediately after the trial, Steve Jackson seemed pretty discouraged. Bill and Pete Kennedy walked across the room to talk with Mark Eckert and company, offering "We've been talking as people to each other for quite some time" - to which one of the Government lawyers returned "Now you know that we're not multi-headed Gorgons; we've all been in the same trench." Maybe not.

Later that night, a number of us met to decompress. We playtested a new game (about post-apocalyptic atrocities rabbits) that somebody had submitted to SJG. Steve wanted to play, wanted to do anything but hear the words "lawyer" and "Secret Service" again for a long time. I brought over a collection of Swords vs Hell game notes for him to check out. When I left just past midnight, Steve was kicking everybody else's bunnies, raising Mormonoids, and studying notes for another game all at the same time. Thus, after standing up in the face of the United States Government, after fighting the good fight for three years without a payback - other than integrity. With all the courage and the humor and the genius shown through, you have to admire a guy like that. Outside the WWII newsreels you don't find many heroes, but here is one indeed.

All cartoons by the author.

As this issue went to press, the verdict in the Steve Jackson case had not yet been reached. It's quite likely that there has been a decision by the time you are reading this. We will leave a recording on our main office line (516-751-2600) as soon as a verdict is announced. Details will appear in the Summer 1993 issue.

One Angry Judge

by Scott Skinner

folly (fŏl'ē) *n.* a costly legal undertaking by an individual or individuals lacking in common sense, understanding, and foresight, resulting in an absurd or ludicrous outcome. [Middle English *folie*, from Old French, from *fol*, foolish from Latin *follis*. See *flo-*.]

We tried. Tried our damnedest to see the trial. Trains, planes, and automobiles: we did 'em all. Even drove halfway across damn Texas desert, to places where even the radio waves don't go, and "TV" is something you catch in a dish. Hell, our while rented compact got wind-whipped off the road so much we nicknamed it "Snowflake". But alas, for us the trial was never to be. "Postponed a week," they said, as we clutched our pulsating hearts. "Heh, heh," they chortled. "That's the legal biz for ya." Yeah, we thought, heh, heh. So there you have it. *Right* place, wrong time. The trial hasn't even started and already we were in the grip of morality.

And just why did we go through all the trouble? Trial's a trial, right? Wrong. For hackers, the Steve Jackson Games trial was nothing less than a religious event; Rome, Jerusalem, and Mecca all rolled into one. It was Woodstock for techno-anarchists, and although our own pilgrimage ended a week short at the gavel, it was not without its moments.

We met Steve at a local Texas bar, and the fury of a hip Austin nightlife. He was surprisingly pessimistic, despite news that the Judge had admonished the Secret Service for trying to sell the case. Still, Steve was anything but hesitant. Cynical, yes. Reticent, no way. "We've waited a long time for this," he said. So we had. It was almost three years since the March 1st raid of Steve Jackson Games by the Secret Service. And three years waiting for justice is a long time by anyone's standards. As we listened to Steve's gloomy trial prospects, we understood that he harbored pessimism as a reflection of the chilling effect the raids and busts have had on us all. Computer enthusiasm and prospects for unfettered global electronic communication seemed dead and gone, replaced instead by a hyperwired hyperparanoid community of closeted dissidents. For many of us, the Steve Jackson trial was the only thing to look forward to. It would hopefully put an end to First Amendment ambiguities that have plagued us ever since the dysfunctional raid against the electronic newsletter, *Phrack*. Through a margarita haze we left Steve and wished him luck. The trial was one week away, and there was nothing left for us to do but slack. Back at the office, we watched and waited.

The trial itself lasted three days. News of the event spread across the Internet so quickly it would have put the AP newswire service to shame (that is, if the AP had even bothered to cover it). The plaintiffs effectively established that: 1) Neither Jackson nor his company SJG were ever suspected of any wrongdoing; 2) There was no investigation of SJG by the SS prior to the raid; 3) The affidavit used by the SS to obtain their search warrant was erroneous; 4) The search warrant did not even meet the Service's own standards for a search and seizure; 5) The work in progress of a publisher was seized, in violation of the Privacy Protection Act; 6) The SS were incompetent, because they were not even aware that this law existed; 7) Electronic mail was seized, printed, and read, in violation of the Electronic Communications Privacy Act; 8) Electronic mail was deleted - evidence was "destroyed"; and 9) The SS purposely and willfully stalled three months before returning seized computers and disks to SJG after the investigation was over.

Incredulous? Outrageous? Judge Sparks thought so, which is why he spent fifteen minutes straight reprimanding Tim Foley (the agent responsible for the raid) for the behavior of the Secret Service. The dialogue that follows is perhaps the highlight of the trial:

Sparks: "Did it ever occur to you, Mr. Foley, that seizing this material could harm Steve Jackson economically?"

Foley: "No sir."

Sparks: "You actually did, you just had no idea anybody would actually go out and hire a lawyer and sue you."

According to the plaintiff's attorneys, Judge Sparks was "visibly angry," and the government was so shaken after being chewed out that they rested their case.

So the Secret Service? They said it couldn't be done. And yet this is exactly what Steve Jackson accomplished with the help of the Electronic Frontier Foundation. If the SJG trial has proven anything, it is the importance of a source of electronic civil liberties protection. Steve was fortunate to have the resources of competent EFF lawyers; many others are not so fortunate. Electronic civil rights activists are needed more than ever. Activists who will not just lobby the government, but go the distance in court against big business, bad law enforcement, and their dated conceptions of First Amendment freedoms. Although the judge has yet to deliver a verdict on this case, we are confident that it will be favorable and precedent-setting. The SJG trial has sent a powerful message to an overzealous law enforcement community: no one, not even the Secret Service, is above the law. We can only hope that, in the days that follow, the Secret Service will take heed of this message before pulling another Foley.

LETTERS OF MERIT

Cordless Questions

Dear 2600:

I was wondering if you know how cordless phones work? I know they have an input and output from the base. But do they all use codes to access their base? I thought maybe some of the older ones didn't and just used a scratch. It would be interesting to find out exactly how they work. I don't know if there's a law on cordless hacking in the Pentagon range? Thanks!

Happy Reader
North Dakota

There is no law against listening to cordless phones. Basically, cordless phones have an radio and some sort of telephone interface and so electronic laws do not protect it. Not only will cordless phones broadcast up to 40 miles from the handset to the base and 1-2 miles from the base to the handset, it is also a very relatively easy to transfer around a neighborhood with a cordless phone and pick up other people's conversations. The cordless industry has worked to become fewer models have frequencies of 46.61 to 46.93 mhz from the base to the handset, 49.83 to 49.99 mhz from the handset to the base, each with ten channels. These models, which have been around for six or seven years, use digital security codes. Some of these have thousands of codes. Others use a system known as rolling security codes, where the code changes with each call. The newest models use 902-928 mhz. Some of these digitally encrypt the audio.

Bypassing Restrictions

Dear 2600:

Recently, my college dorm installed a Sprint long distance calling card program in which a five digit code must be entered after dialing 9+11 area code+number. Being the curious guy that I am, I wondered if I would be able to get through to 900 services without being routed through the Sprint service or denied calling altogether. As it turns out, the first time I tried it, it worked without going to the tone for the phone code. After that, it wouldn't work. I keep getting a message saying that the call couldn't be completed and an operator would not be able to help (weird). My question is: why does it work sometimes and not the other times? Recently, I have been able to get through to the same number (Dungeon, for instance) with it working.

Confused
Major Tom
Champaign/Urbana, IL

There are many reasons why this could be working sporadically. It's certainly quite possible that certain portions of security can be bypassed depending on which carrier(s) the call goes through. If this is the case, you can be assured that the software engineers already know about such bugs. Perform some experiments - see if the results vary during busy hours, days, etc. Compare with other cordless phone users in your area. It's possible any number might work if there's a trick we don't know about. Remember that it's also quite likely that everything we do is being recorded somewhere.

More Simplex Stories

Dear 2600:

Apparently someone has been applying their knowledge of S-style locks, especially on FedEx lockboxes in the Boston area. Apparently, FedEx is less than happy about this, and has taken measures to put an end to the robberies. If it were me, I'd do something about the locks. But it's not, and FedEx designers welcome. They've gone to the police and gotten them to "stakeout" a number of FedEx lockboxes (the ones being robbed, I guess). But they have not (yet) changed any of the numbers on their lockboxes (I checked - call the screen). I don't know if UPS has done the same, or whether the thief has even bothered to take from them. I personally have seen no instances of lockouts on UPS. Their boxes continue to use the same combination.

A Fly on the Wall

It's incredible how stubbornly some companies will cling to their customers.

Dear 2600:

I recently saw a push-button door lock made by Best Lock Co. that looked identical to the Simplex Series 1000. Are these Best locks as unreliable as their Simplex counterparts? Can each number only be used once in the combination, thus reducing the number of possible combinations?

Pez
Lafayette, LA

Best does not make publication sales. What you probably saw was a Simplex lock with a Best core. Some Simplex models have key bypasses and the keys can be made by any company.

Mysteries

Dear 2600:

Recently, I stumbled upon a program called MCI VoiceLink v5.1. It runs under the Unix operating system. I have thoroughly investigated the actual VoiceLink program, and still have yet to figure out what its main purpose is. I've heard descriptions ranging from "a long distance billing maintenance program" to "a simple voice mail program." Judging by the name of the program, I am inclined to believe the latter, but am still unsure. Any help on this issue would be greatly appreciated.

Annnie

A lot would depend upon where you found it. But it's not even necessary to access the Unix to do a lot of covert activity. Call the friendly folks at MCI sales and ask them for references. We doubt they want to keep it a secret.

Dear 2600:

I was wondering if you could answer a question I have about the set of numbers I discovered. There are four numbers I found with the same message on them - in two pairs of two. There is no ring-tone when connected, and the receiving quality sounds like a Voice Mail service. The numbers are: 0800 875 857, 0800 871 871, 0800 879 879, 0800 875 860. When connected, you hear this: "This is an SEC test number. Please enter the CSU [could be CIO - it's not clear] you wish to simulate." Then it accepts 10 digits and either gives a continual tone (disconnect) or an engaged tone (number). So, what is it? I don't know if it's important, but is the answer connected to the fact that each pair is right next to each other? Hope you can help. Incidentally, could you tell me if you know of a UK magazine similar to 2600?

DG
UK

We know of no magazine like 2600 in England. If anybody figures out what mystery numbers, we'll print the answer here.

Dear 2600:

While scanning my local exchanges, I've come across a few numbers that seem to cut voltage to the line for about 15 seconds. For example, after dialing 317-646-9694 the line dies and even attempts to produce normal DTMF tones result in silence. Do you have any idea what this exchange is? Incidentally, ANAC for 317 is 2002002020.

Mastatron 317

It sounds like another phone company test number. Assuming that your voltage meter worked okay, and testers in the 90's or 00's were is almost certain to be telecom-related.

Hacking Passwords

Dear 2600:

I have a 2600 issue from Summer 91 which talks about a Unix password hacker. It doesn't give the source code or any real info, because it was given in a more previous issue of 2600. Where can I find this "password hacker" and the source code? Is there a VMS VAX equivalent also?

MR

There are lots of password hackers out there. The best one we know of is SUPERUFF.XXX, which comes out of Holland. There are many more that are designed to run on different types of computers. Obviously the more powerful the machine, the quicker a password hacker will run. By searching around on bulletin boards and the Internet, you should be able to find some of these programs. Unix systems are such popular targets because, unlike other operating systems, the password file is easily readable (with the exception of those systems that use shadow passwords). It is not hard to read this file. It's also not illegal to run a password hacker on your own computer, perhaps you didn't obtain the password file illegally. Actually using a guessed password to obtain

access to a computer you are not authorized to use is illegal. Be careful.

That Bell Computer

Dear 2600:

You guys really pissed me off with your Telco News Winter 92-93.

What a stupid thing to put in your mag! It's been well known among the hackers for years that most security is overlooked and in some areas blatantly ignored. Writing about one particular company's security weaknesses is a direct slap in the face. As a result, that company will be highly pissed and most likely take procedures to tighten up security. But you're defeating the whole purpose of hacking: learning! How much information could have been learned from that one particular system? It's hard to say. What do you do though instead? "Oh, hey let's put it in 2600 so we will show them how stupid they are." Did you ever think that you might be ruining it for the other hackers out there that are trying to learn about the phone company's computers? Nah, I don't suppose that even crossed your mind. The article was lame anyway to those of us who know what's going on. Most of that shit was information found on the Bell Newsletters. Of course the phone company is gonna say that hackers cost them money. They want the general public to keep believing in the same "Hacker Hood" image that *Forbes Magazine* proudly wrote about. It should be obvious to you that after the 911 incident with Neidorf, the embellishment of things damaged or costing money was part 98 made up to make the hacker look bad, malicious, or anything but the truth. I just lost a lot of respect for 2600 when you printed that. Hah! Not that that matters much anyways. I don't think you guys ever did any real serious hacking. Otherwise you would be working on some covert projects instead of publishing a magazine that keeps all the security people up to date on what we are doing or things we have uncovered. My main point is: a hacker would never tell an admin what holes to patch if he wanted to continue hacking the system!

So why are you?

Iagden82

First off, we print information that we feel deserves to be shared. We don't advise over what the courts will do with it, whether they may happen to it. If we did, we'd probably never be able to print anything. As far as your "concerns", let's get a little real. We're talking about a major computer system that has a wide open front door, isn't it? Who would we be serving by keeping that to ourselves? Something along these lines is not too bizarre for our issues. And, sure enough, at least one of our readers was able to provide some valuable insight into this (see next letter). How we choose to print our info is up to ourselves and on the whole like you "who knows what's going on", this automated hacker info would never have been able to exist.

Dear 2600:

Enclosed is a copy of a Pacific Bell system

login. As you can see, after six attempts, anything will log you in. This is identical to the SouthWestern Bell computer mentioned in the Winter 1992-93 issue. Apparently it's some kind of standard RBOC hacker trap. Does the word escapenet spring to mind? Either way, the worm never actually broke into the SouthWestern Bell computer and neither will anybody who calls the number you listed. They'll simply fall into this false dial tap.

The Road Warrior

Thanks to you, our writer has now come out of hiding. The printout you sent us was almost completely identical to what we had printed. Considering this comes from another RBOC, this may be a standard ploy for many phone companies. Our next question is what are they doing with these traps?

Correction

Dear 2600:

The frequencies given in "Defeating Callback Verification" (Autumn 1992) for the dial tone are wrong. After many hours of picking up the phone and listening to the dial tone, I decided that the correct frequencies were 350Hz and 440Hz.

CA

Georgia Tech

We stand corrected. For a collection of correct frequencies, you can refer to the Summer 1992 issue, page 12-13.

Info

Dear 2600:

Here is a tidbit you may want to share with your readers. For AT&T calling card kids you can without any surcharge from any phone (work, hotel room, etc. for 10 cents a minute under the following conditions: 1) You subscribe to Reach Out America ($10 month includes one hour of free calls/mo. off-hour calls). 2) Your call is made to a number which is in a different area than the one you are calling from. 3) You call off-hours (weekends or 10 pm to 8 am).

Concerning the ongoing issue of lack of security and verification provided by various institutions (banks, telephone companies, etc). I lived for many years in European countries (Ireland, France, Switzerland, Great Britain), where you are not trusted by anybody. Every action requires positive verification. This may prevent some errors but it makes life very difficult for crackers who do not want to abuse the system. Missing a rollout call or third party call takes twice as long because everything has to be verified. All contacts with authorities have to be done in person as nobody trusts a phone call. Even a letter is suspect. Coming to the United States, where you are to ground trusted by the authorities, was a big relief.

CL

Philmont, NJ

While the AT&T plan is better than nothing, there are still far too many restrictions. Why we need an interstate, coast-to-coast, real-time way for all of us to make cost-free calls from any place in the country. Any phone companies out there interested?

Dear 2600:

We have a quantity of surplus touch tone desk phones, including the five-button model. We would like to export them to the Ukraine. Pulse is necessary - is there an in-line converter from touch tone to pulse or tone? Sounding for would be an inexpensive add-on!

JR

Kingsburg, CA

We know of no such device that's already constructed. Basically, you'd need a touch tone decoder to convert the signal to pulse. It's not of like converting a tone to voice.

Dear 2600:

Here are some phone numbers that go to a modem computer running the MIX LDX system: 602-941-3816, 2617, 3782, and 7783.

They are on an EDI system used to transfer IGES engineering design files. Don't be surprised if you see classic Genisolve guidance systems in them.

The Tick

Arizona

Two things surprise us anyway.

Dear 2600:

Greetings! Your readers may want to know about the magazine *Midnight Engineering*. It's loaded with articles about single-board computers, microcontrollers, embedded systems, etc. The latest issue has an ad on page 62 for "Spy Supply" and advertises a "cellular telephone modification handbook" for $79.95. Looks interesting. One of your recent letters asked about cable TV hacking. Here's some info. Most of the current models of descramblers are digital. There's all sorts of internal monitoring software in these boxes. A friend of mine works for a local set-top manufacturer and gave me the scoop. These boxes can detect tampering and have programmed in "panic" levels. If you mess with them, they'll shut off, but if you undo your wrongs, it'll forgive you and start working again. If you really mess with it, it'll write alternating 1's and 0's into its program store and die. The way they catch hackers is something like this: the control office for hotspot x periodically sends out a signal that says "everyone now getting HBO, raise your hands" and the set-tops do it. Then says "I will now read a list of everyone who's supposed to be getting HBO. As I call your name (ID), you may lower your hands." When the roll call is done the signal is then sent out "everyone who still has your hand up, please self destruct." Kablooie. It's sad (?). Here's a fun hack: stretch out those "free preview weekends". The cable company sends out a signal that says "tell non-privileged set-tops, turn on HBO" and you enjoy the weekend. They then send out a signal at midnight Sunday: "OK, turn off HBO." Suppose your set-top gets the turn on signal and somehow gets unplugged from the cable system while the turn off signal is being sent. It wouldn't know it wasn't supposed to not be getting HBO when it was reconnected sometime Monday. A friend of mine tried this and even called the cable company to report that he was still getting HBO. They didn't believe him and never did anything about it.

Gentle editor, I have some experience with what the local BOC calls ESSX (out of service). The most interesting part of this is the customer is allowed into a database to reprogram his phone features. Yes, Ma Bell actually encourages customers to do this. If you think it would be of interest, I could knock out an article on ESSX hacking.

Avatar

We're certainly interested in another title for the one you suggest. As for cable, check out page 16 for more info.

Dear 2600:

In your last letters column was a request from a reader on a magazine called *Mobile Office*. I got it at the office, so here's the info. Subscriptions can be placed at (800) 621-5231. Letters to the editor can be addressed to 21800 Oxnard Street, Suite 250, Woodland Hills, CA 91367, FAX: (818) 593-6152 CompuServe ID: 76648,1722. I found your magazine on the rack at the new Jack London Square Barnes & Noble. I had heard about it back on the West and in other publications.

Ken

Dear 2600:

I think someone a while ago asked about those stand alone credit card readers/dialers. I got an old VERIFONE, and we also use a new model where I work. The password to get into them is 166831 (I think some of the new ones replace that with 266831. I haven't totally got it figured out yet, and there are a lot of differences between the old and new ones, but if you're interested I'll get back to you. There are some big registers in there that I think control it by using 166. I know the one I have can go into a diagnostic mode by hitting * and 3 at the same time, giving you four diagnostics to choose from. Choosing 4 lets you swipe a card and read whatever's on it.

Misha

Dear 2600:

I've found out some interesting stuff on the ever-popular Radio Shack tone dialer conversion. According to the original article (*2600*, Autumn 1990), the optimum crystal frequency for creating red box tones is 6.498 MHz. As shown in that article, a 6.7936 MHz crystal would work. However, I noticed that Digi-Key (800-344-4539) sells extremely small 6.500 MHz crystals, so I tried one in my tone dialer. It works great, although the timing of the tone pulses is audibly different than a real quarter tone. I installed this tiny crystal inside the dialer, along with the original 3.579 MHz crystal and a mini slide switch. If you want to try the 6.500 MHz crystal from Digi-Key, get part number X415. Only cost $1.53. I also noticed that the dialer can generate a single-frequency tone. I'm talking about the "error tone" that beeps at you when you enter an invalid key sequence. This tone comes out of the little piezo speaker rather than the large main speaker. You can keep the tone sounding by pressing the "memory" key twice, for example. The pitch of the error tone changes with the crystal frequency of the dialer, just like the DTMF tones do. I was curious as to how the pitch (or frequency, if you will) of the error tone was related to the crystal frequency of the dialer, so I checked it out in the electronics lab. I found that the frequency of the error tone is equal to the crystal frequency divided by 1024. For example, if the crystal frequency is 3.579 MHz, the frequency of the error tone is 3579000/1024 = 3.495 kHz. So if you wanted to generate a certain single-frequency tone, like 2600 Hz for instance, the necessary crystal frequency would be the desired tone base frequency times 1024. For 2600 Hz, the crystal frequency would be 2600*1024 = 2.6624 MHz. Unfortunately, this is not a standard crystal value. With all this in mind, it would be very convenient to have multiple and selectable crystal frequencies for your tone dialer. If anyone could come up with a low power, stable, variable frequency oscillator which was controllable from the dialer's keypad, that would be a major hack.

Mr. Upsetter

Red Box Questions

Dear 2600:

Is there a known incompatibility with red boxes and Pac Bell payphones? I've tried it on Pac Bell payphones all over town with no joy. A friend suggested that Pac Bell may have tweaked the tones a wee bit so as to render the red box trick useless.

I wish that I had looked in the back of your mag before ordering from JAN crystals! I could have saved a few dollars building a device that may only be of use in other parts of the country.

Frustrated in Berkeley

There are two types of calls that will accept red box tones. One is for inter-LATA (as you call Pac Bell) calls (not local calls that don't require an additional deposit). The other is for calls handled by a long distance company. There are two different systems so what doesn't work on one may work on another.

Data in the Air

Dear 2600:

I have two questions. First, I have recently bought a $20 radio transmitter from a mail order place that advertised in the back of *Popular Science*. What I was wondering about was, would it be possible to send data from a modem over the airwaves via the transmitter? And just have the people listen in, connect their modems to a radio receiver, and watch as the data is fed onto their screen. Next, could you settle an argument I am currently in with my friend. On New Year's Eve, while my friend was phucking with a payphone, and we were waiting for a ride to pick us up, I tried to explain to him that television cable was transmitted over the phone lines. He doesn't believe me, and although I do believe I read it somewhere, I am not certain either. Thank you, could clear things up for the both of us?

The Winged Placenta
Oregon

It certainly is possible to transmit data over airwaves. WBAI FM in New York did this a number of years ago. Of course, most listeners felt compelled to change the station at that point. If your transmitter is delivering a clean signal, you should be able to do the same thing, however your range will be very limited. Cable TV can only be transmitted over phone lines if the phone company controls cable TV. It's considered the norm of the future to have this happen, as well as to have cable companies delivering alternative choices.

Questions

Dear 2600:

In your current issue, in response to a letter for books to read to better understand telecommunication systems, you list *Telecommunications System Engineering* by Roger L. Freeman. I have accessed my local library's computer network (which is connected to about every library system in the northern part of Ohio), and found only one location with this book. They have it listed as a reference book, which means it cannot leave the library. This library is not anywhere near to me. What I would like to know is if you have an address to the publishers or someway that I can get a copy of this book? Thank you. And keep up the great work!

JG

That book is readily available in bookstores. If you need to contact the publisher, they are Wiley-Interscience located at 605 3rd Ave., NY, NY 10158. The ISBN number of the book is 0-471-63423-6.

Dear 2600:

In the book *Out of the Inner Circle* the author mentions that in 1954 the Bell telephone system published a complete description of the multifrequency system, including the specific frequencies and descriptions of how the frequencies were used. Is this information still applicable today? Hasn't the phone system done anything to stop the use of blue boxes? Can I get a copy of this article somewhere?

TW
Binghamton

You can probably find that Bell document in a technical library somewhere but you can get the same information in any hacker publication, including this one. And, yes, the phone company has done quite a bit to stop the use of blue boxes. The victims are really over.

Dear 2600:

Is the $260 lifetime subscription retroactive to all back issues?

MJ
Massachusetts

Yes, but as of now, all lifetime subscribers also get 1984, 1985, and 1986 back issues. (No advertisement). Current lifers can write us if they want to get these issues.

Dear 2600:

It would be greatly appreciated if you could answer a few questions for me. First, does AT&T or any third party sell operator or service manuals for telephone switching systems? Second, how does one find out which switches are where? Third, what frequencies do cellular telephones transmit on? Finally, is there any way to tell if ANI is being used on you?

SB
Massachusetts

You can get phone company related manuals from the AT&T Customer Information Center at 800-432-6600 or Bellcore at 800-242-2121 or 908-699-5800. We should warn you that they can be rather expensive. For a free guide, ask for the catalogue of technical information. As for finding switches, it requires a bit of skill. You have to find someone in the phone company who can tell you, which can be amazingly difficult. All the cellular info you could possibly want can be found starting on page 4. ANI is always being used in some state - operators and the billing computer always receive this information. It's wise to assume that all 700, 800, and 900 numbers are using ANI.

Dear 2600:

What issue contained the article "How Phone Phreaks Are Caught"?

Also, I built a red box and use it on businesses when I'm on the road. I've used it on a couple of payphones by my house. Is this wise? What are the chances of getting caught?

Finally, does anyone monitor what goes in and out of the *2600* offices?

Freakel-out Feyodor

That article was in the Spring 1990 issue. But if you keep it up, you may be writing the sequel. Most beavers of the past were caught primarily because they used the same phones, often ones inside their homes. Red boxers can only use payphones but the same logic applies. If a phone is abused enough, it will be monitored at some point. And if you happen to be a snoop in the neighborhood, it could get unpleasant. As for people monitoring our traffic, we have no way of knowing. But we do know that sorting and nobody comes into the office is unknown and unheard.

Dear 2600:

There used to be a three digit number in New York City that one could dial, hang up, and get to ring in your own phone. I had used this several times years ago and learned that the number is changed regularly. I contacted a New York Telephone techie a few weeks back who advised me that this phone capability has been discontinued. Since I cannot take this as gospel, I am hoping that you have that "secret" way of getting your own phone to ring without having to ask the other reluctant operator to do the same. This capability is useful to me when I wish to check out my somewhat defective Color-A-Phone answering machine.

Also, perhaps you can tell me where I might purchase the removable carbon pile mouthpiece that slips into the "talk" end of the handset. It has no wire connectors and makes contact by pressure alone. The phone company will not sell me one. (The carbon in the piece evidently takes up. Tapping it on a table can raise but mine is tapped out.)

AB
New York

The prefix 960 plus the last four digits of your phone number works in much of New York. After getting a second dialtone, you flash the switchhook, hang up, and your phone rings. An alternative way of getting a ringback is to subscribe to 3-way calling. While connected to something (preferably toll-free), flash once to your 3-way, then hang up. Your first call will ring back. As for getting a new mouthpiece, go to where old phones are found. Yard sales are one place where you can find old phones and their components for virtually nothing.

Dear 2600:

In the Winter 1990 issue (page 28) there was a request for development of a circuit or "add-on" box to send a false number to the party you are calling through Caller ID. Has any such animal been developed or are there any such plans in the works?

JL
Shoreham, NY

We hope there are plans but we have yet to see them. Are readers out there interested in doing this?

Dear 2600:

I play guitar in a ska band in New York City and know a bit about the origins of the music. I noticed a cover a while back done by a "Sir Lord Comic", who was a ska scatter in Jamaica back in the '60s. I have little doubt that the Sir Lord Comic who penned the cover knew of this, but I just had to make sure it wasn't the original. No way, but I had to ask. And another cover with reference to a Bob Marley song made me have to ask. I love *2600* incidentally, keep it coming!

Recording

You're very observant. Sir Lord Comic was not the name of the artist who did the cover even though it looked like a signature! It was a reference to the very person you recognized. Lawless Street was another reference to a ska song of that era which appeared on the same cover.

Fixing Your Credit

Dear 2600:

Just picked up the Winter 92-93 issue. The enforcement of the Fair Credit Act comes under the jurisdiction of the Federal Trade Commission. That's why the "police" wouldn't help payoff. He has to write to the FTC. And yes, Motorola did violate the law big time. He may also write his Senator and Rep. about the problem. If all they do is write a letter on his behalf it can be enough! If AMEX gave Motorola a card in his name without having his signature on an application, then they are in the big doodoo - once again FTC's jurisdiction. For anyone else having credit problems: first talk to the person who put the stuff on the report. Many times they can be dealt with (if you are nice and they are not). If the bad stuff is from Sears, it may take a personal visit but many car dealers/mortgage companies know that Sears is the worst and will completely disregard any negatives from them. Next step: have the creditor contact the big three (TRW/Equifax/Trans) or contact them yourself via letter (always certified with return receipt requested) and point out the error. They will investigate and get back to you in 6-8 weeks. Most problems are solved at this point. If you still have a problem with a creditor validating a bogus debt about you, call them or write them one last time and ask them to produce the evidence (the credit slips you charged but never paid for). If they can't and they don't remove the debts, write the FTC and complain. A lawyer is the last step. Most often you don't need one. You can after all file a suit PRO-SE (on your own behalf). Sometimes though, as I said, a personal visit to the credit office of whatever is the pain in the butt will help immensely. Get their phone number and call (or visit) a library near them. Look in *Color* (reverse directory) for the address. Usually the actual number will not be there but you will find a number close which is the start of the block for their PBX. Now you have the address. Get into a suit, clean up, cut your hair (just kidding, but it works!) Give 'em an unannounced visit. Don't take "she's in a meeting". Be firm, but polite. Stick up for yourself. This procedure clears 95+ percent of incorrect (and bargains away 75 percent of correct) derogatory information from your credit report.

DC Central

Surprising Facts

Dear 2600:

Have you seen these numbers from the phone companies? The major telecom carriers are reporting that 1992 was a bad year for the phone bubbles intent on ripping off phone service from corporations. Sprint reported fraud claims by its business customers down 90 percent, to $670,000, or $1,150 per incident compared to an average loss of $55,000 in 1991. AT&T says fraud claims made to it dropped about 88 percent, and MCI says it has also seen a drop in claims. In other words, 1992 losses were a far cry from the $1 billion to $3 billion a year claimed as losses in past years. The major reason for the drop: customer awareness.

JM

Meanwhile the number of hackers continues to rise.

Spanish Connection

Dear 2600:

I would like to collaborate with *2600 Magazine* and send articles and present information from Spain. There are very many people interested in hacking at

Spain and Latin America.

Here is some interesting information:

Criminal Justice Bulletin Board Services: 602-236-1609, 415-614-6806, 408-267-8599, 916-392-2550 (NCJIS - SEARCH), 818-405-4242, 714-534-8931 (APCO), 310-915-3735, 510-925-9057 (DALMP), 719-591-3415 (FIRENET), 303-987-7368, 904-646-2775, 301-447-2747 (Arson BBS), 201-738-8855.

My hacker group is IBURFACKEZ.

GMV
Motril-Granada, Spain

BBS Info

Dear 2600:

I was wondering if there is some sort of BBS newsletter to keep me informed on BBS comings and goings, which are hot and which are not, etc.

JCB
Concord, NC

Boardwatch is probably the best. You can reach them at 800-933-6038. For those outside the U.S., dial 303 973-6038. If we hear of others, we'll pass them along.

Evil Payphones

Dear 2600:

I have noticed an annoying and disturbing trend in my local C&P Bell payphones. They have started to act like COCOT's. I first noticed it about six months ago, when a new legion of C&P phones with gray leather (not black) handsets started appearing. I placed a local call on one of them, using a quarter, and I could hear this little click a few seconds after the call went through that sounded as if they had just activated the speaker (it turned out this was true). Odd, I thought. Then, after three rings, this computerized voice came on and said something like, "Your called party does not seem to be answering. Please hang up and try again later." I was very irritated at first, because I thought it had disconnected me and would not even let me leave a message, but it in fact did not disconnect me. Nevertheless, this genuine C&P Bell phone acted exactly like a COCOT. Is it possible C&P is buying up COCOT's and converting them to C&P phones? The phone looked exactly like a standard C&P payphone, except that the familiar black handset was conspicuously gray. As you can probably guess, red locking off of these new phones is as difficult or impossible as it is off of a COCOT.

I called C&P to ask them about this, but the woman I talked to knew nothing about any new C&P payphones. She thought it might have been related to their new Send A-Call feature, which they apparently have been having a lot of problems with. But that didn't make any sense. This particular phone did have a plate below the instructional plate describing the Send A-Call feature, which I hadn't heard of before, in place of the usual plate that says "Out of Change? Place a collect call, etc."

Infoman
Arlington, VA

Nothing is impossible when it comes to phone company phone. The best example of this is AT&T's arming people and in one weird instance payphones nervous they'll rip you off. Of course, in more than a few instances, if you take a good look at these weird looking payphones, particularly the ones that try to look like "regular" ones, you'll find that they're made by AT&T.

Access to 2600

Dear 2600:

At last I've found a niche. After being confused beyond belief by those goons at *PC Week* and perplexed out after thumbing through the pages of *Macworld*, I've discovered that *2600* is where I belong.

I was at a bookstore, looking through gaming mags. Between a seriously misplaced *Better Homes and Gardens* and a very outdated *Electronic Gaming Monthly*, I saw a thin page with the remnants of what looked like the numbers 2600 on it. Underneath this was printed "The Hacker Quarterly". My curiosity then got control of my body, and I investigated it open. Despite the crappy condition, I paid the four bucks. When I got to the counter, the clerk told me that the store would stop carrying *2600* with the next issue. Looking at my copy, I see that it is the Autumn issue. No doubt, by now the winter issue is out and I have no place to look for it! At any rate, I sat down that night and couldn't believe what I was reading. All this talk of telephone "tricks" with the use of electronic modems made me think to myself, "Shit, this is cool stuff and I want more!" I'm now thinking of subscribing. I just have one question. How come a one year subscription costs 21 bucks, when cover price is $6?

Read Peter's article on getting started really spurred me on. Being an extreme beginner, I have little or no knowledge of these "hoses" that everyone seems to be storming in. You should make a "guidebook" available for the price of a back issue. This book should explain what all normal readers are assumed to know, so that we (new readers and novice phreaks) don't go into thinking blind.

Kudos to Count Zero for his info on COCOT's. With his article, I was able to successfully build a zombie box by making enhancements from existing Radio Shack tone dialer. I had a hell of a time getting the materials, though. It would appear that Radio Shack employees are very reluctant to look over their wares unless they know what they're going to be used for. When they see a fourteen year old getting a pocket dialer, a mini toggle switch, and a little bit o' wire, something must go off in their heads. My conversation:

Radio Shack Techie: So you're into phones, huh?
Me: Me? No, not really.
Radio Shack Techie: Well, why're you getting this?
Me: It's (insert) a Christmas present!)
Radio Shack Salesperson: For who? Your dad!
Me: (go to hell) No, my friend wanted me to pick it up for him; I don't know why.
Radio Shack Techie: Well, you could do some pretty scary stuff with this thing if you know how to use it.
Me: :)

Radio Shack Salesperson: Well, there ya go. Have fun.

Crap, ya? Is it really necessary to ask all of those questions? I was afraid that if I reminded the man that it was none of his business, he would forget about the sale that was in effect that day.

Please write back your response, because I doubt that I'll be able to read about it in your mag. Under the circumstances, I don't think I'll be able to find *2600* as easily as I did last time.

The Apple II Evangelist
Palos Verdes, CA

Your problem is very easily solved. All you have to do is subscribe! It costs a little less to get us on the newsstand but there is that degree of uncertainty that you have to go through. Regarding Radio Shack, we don't know why they have to interrogate all of their customers the way they do. It's extremely annoying and has led many of us to go elsewhere. On those rare occasions when we have no choice, we always feed them bogus info. A little thing like an eight digit phone number or a zip code with a letter in it can ruin their entire day.

Rolling Stone Corrections

Dear 2600:

Reading the Autumn 1992 issue, I read through Clark Kent's nice letter on the hacker's reading list (page 28). I stopped over and picked up a copy of the *Rolling Stone* September 19, 1991 article "Samurai Hackers" and got an instant laugh.

If you'll recall the *2600* article (Winter 1990) which the *Stone* author (Lycia Edwards) cites, it wasn't at all as what she had written.

1) I am not a GOP staffer.

2) I was definitely outlined by Jeffrey Laud.

3) Laud did not like any hackers – rather, he was one of them and it was his opposite number. I was only hired to do so – hence my term, "Samurai Hacker" (in memory of John Belushi, who I hope is enjoying this even as I write). In point of fact, this was the point of the article – a reference of how hackers, like the samurai of old, often work under the auspices of indifferent or ignorant powerful lords and political figures.

4) Laud was soon exonerated after the legislature hearings. Although ample allegations of corruption and governmental abuse were uncovered, both parties simultaneously excused the other. Laud now works as the Deputy Register of Deeds for the County of Camden. He now makes nearly $5,000 over what he previously made as a legislative staffer.

5) And for the closing act, read the Asbury Park Press - July 25th, 1991, editorial page A-18 on the matter of the media computer tapes being destroyed. It was, you see, the discrepancies which appeared in the master tapes which led the entire investigation in the first place. Little or no mention elsewhere has been made of these records being destroyed.

Aside from good soldiers being scrambled, so what?

Sometimes media topics bother just that – topics. I find it amazing when a large scale mass marketed magazine as *Rolling Stone* can't even get verbatim what it is they're doing correctly. (I suspect that Ms. Edwards got her information verbally, rather than from a direct source.) If this is the case, then how can these guardians of democracy report responsibly as to what is actually going on? I agree with Mr. Goldstein's position that the media must themselves be better informed and that we had better start making sure that all aspects of The Word is put out there for all to consider and judge accordingly. Dialogue must continue as we much as is safe for us to keep quiet.

What good is knowledge if it's wrong?

Keep the faith, Jolly.

TEL Ejectable!

We couldn't agree more. And to answer your private question, the answer is yes.

Special Phone

Dear 2600:

Where can I buy a phone that has the A, B, C, and D keys on it in addition to the 0-9, *, and # keys? My two most annoying radar has them on it. But I can only use them when I am making phone calls via an auto-patch.

JT.
Tempe, AZ.

Modems are also capable of dialing the extra five keys. If anyone knows of regular consumer phones that have these keys, we'd like to know. It would add some extra security to voice mail, answering machines, and the like.

Seeking Virus BBS's

Dear 2600:

I just received my first copy of your magazine and love your back issues, and I love them. I don't know if I'll ever have the guts to climb up telephone poles and do late night hacking sessions, but I have been known to poke around a few Internet sites and have a look. Your publication has already given me ideas on some new fun things to try.

I'd like to know a few things: 1) Do you or your readers know how I could get into any of the virus BBS's that are out there? Every time I read an article on viruses I keep hearing about the "useful BBS's" that carry virus source. But I'll be damned if I can find one. 2) Are there people in the Rochester, NY area that would be interested in having *2600* meetings? I'd offer to try to set things up myself but I travel quite a bit and my attendance would be sporadic.

Maybe if I find some European virus BBS numbers I'll have a good reason to build the Radio Shack red box and do my BBSing for free!

YFNH
(Your Friendly Neighborhood Hacker)

There probably are people in your area interested in having meetings but somebody has to take the initiative. There are BBS's that specialize in viruses but they're kind of funny about giving their numbers out. If you succeed in your quest, you will certainly be a sight: a hacker with a laptop hooked to a payphone using a red box to connect to a European virus BBS. You just can't get more evil than that.

Cellular Magic

(continued from page 11)

825.990	825.960	825.930	825.900	825.870	825.840	825.810
825.780	825.750	825.720	825.690	825.660	825.630	825.600
825.570	825.540	825.510	825.480	825.450	825.420	825.390
826.420	826.390	826.360	826.330	826.300	826.270	826.240
826.210	826.180	826.150	826.120	826.090	826.060	826.030
826.840	826.810	826.780	826.750	826.720	826.690	826.660
826.630	826.600	826.570	826.540	826.510	826.480	826.450
826.990	826.960	826.930	826.900	826.870	826.840	826.810
827.780	827.750	827.720	827.690	827.660	827.630	827.600
827.570	827.540	827.510	827.480	827.450	827.420	827.390
828.360	828.330	828.300	828.270	828.240	828.210	828.180
828.150	828.120	828.090	828.060	828.030	829.000	829.970
829.940	829.910	829.880	829.850	829.820	829.790	829.760
829.730	829.700	829.670	829.640	829.610	829.580	829.550
830.520	830.490	830.460	830.430	830.400	830.370	830.340
830.310	830.280	830.250	830.220	830.190	830.160	830.130

Monitoring of the base sites is obviously going to be easier than monitoring the mobiles. The cell base sites are towers (usually blue) with a triangle shaped "head" on top and sporting a couple of what appear to be vertical antennas. These base sites have a range of three to five miles. If you take a look at the honeycomb diagram, you can see how they are laid out. The cell transmitter is in the middle of the cell. It is possible to hear many, most, or all of the cells in your city, depending on your location. The closer you live to a boundary, the greater the chances of your being able to receive more cells. Due to the nature of radio signals, the actual cell shape is more or less round. However, the hexagon shape lends itself better to show how the system is laid out. With a circular coverage area, there will be some overlapping between adjacent cells.

If, for example, you live near the asterisk (*) in the above diagram, you will be able to easily hear the G, C, E, and A cells you're near. Since the maximum practical range of a cell is three to five miles, you'll be able to hear them a bit farther away. However, due to the nature of the FM transceivers at the cell sites (they capture only the strongest signal), you should be able to hear all seven cells. Which one of each cell you hear will depend on your location and the strength of the received signal. In the above diagram, you'll most likely hear the F cell in the upper right, rather than the one on the left.

Mobile reception is almost a waste of time unless you have an outdoor antenna. And, since the mobile will be reported on the cell site, it's better to listen to the cell frequencies. You may not be able to hear both sides of the conversation if you listen only to the mobile frequencies. It is useful, however, for determining which channel cell you're in. If you use the antenna that comes with the scanner, mobile range will be decreased down to one or two miles. By checking the scanner readout against the cell list above (825.030 894.960 MHz), you can tell what cell the mobile is in. This is also useful on the cell site frequencies. If you hear someone say, "I'm at the corner of highway FF and 33," and you know where the cell site antenna is in that area, you can check the frequency listing above and determine what cell that antenna belongs to.

Where to Get What You Need!

Obviously, a device is needed to download all those ESN/MINs etc. off the cellular airwaves. Here's the stuff I found so far that is under $2000 (this ain't a cheap hobby).

CCS Company, P.O. Box 11191, Milwaukee, WI 53211 (414-781-2482) They sell everything you need for $300 to $400. Kits are cheaper. Their device interfaces between an 800 mhz capable scanner and your computer. Make sure you tell them you want the REVERSE model DDI. (This is what I use.)

Curtis Electro Devices, 1235 Pear Ave, Mountain View, CA 94043 (800-332-2790, Fax 415-964-38741) They sell an ESN reader for $1295 that can read ESN/MIN, etc. but only from a short distance (maximum is 50 feet). They also sell a security model for $1595 and a NAM programmer for $1195. They publish a book called NAMFAX for $179 that tells you how to re-program hundreds of different cellulars through the keypad on the handset. (Note: You can't reprogram ESN's through the keypad unless you re-write the phone's software.)

Wavetek Communications Div., 5808 Churchman Bypass, Indianapolis, IN 46203-6109 (800-345-6366 or 317-788-5965) They sell a "Cellular I.D. Tester" that's real similar to Curtis's ESN reader but supposedly has a longer range. Price: $1495.

Needham Electronics, 4539 Orange Grove Ave., Sacramento, CA 95841 (916-924-8037) They sell screen burners for $129.95 (I bought one myself).

Motorola (800-455-5202) They sell a cellular service manual that's used in their cellular service classes for $30. Ask for the Order Fulfillment department: Item # 68-P81150E60. This manual tells it all. An absolute must to have.

Bishop Company (800-829-0572) They publish books similar to Curtis's Namfax. Send for catalog.

Cellular Security

Well, we know a properly cloned cell phone is virtually impossible to detect. Or is it? Security companies rely on matching call patterns of subscribers' histories to current use. I.e., when 200 calls to Egypt show up in a day or 80 long distance calls to Colmon, Alabama show up in a short period, all kinds of flags and whistles go off! The security companies will even keep records of people that call numbers that have been previously called by tumbled phones and flag the phone calling that number as a potential fraudulent phone. These flags can be set to go off by a number of parameters: number of long distance calls per hour/day/month, etc. Another method they use is when the real phone places a call and the tumbled phone places another call soon afterwards, but from a distance from the first call that's impossible to travel in such a short period of time. Example: At 5 pm Friday Phone A calls from Manhattan and completes call at 5:10 pm. At 5:12 pm Cloned Phone B calls from Queens. No one can travel those distances in two minutes, thus that ESN/MIN is tagged as a clone by the phone company. These catchers are just now starting to be used in larger cities. Some software will track a flagged cell phone from cell site to cell site.

Common thieves/novices cell company software looks for the different ESN's, manufacturer, model, SCM's, etc. that are broadcast by the cellular phone on its REVERSE channel. (If one captures all that data off the reverse channel and compares it to the cloned phone, detection via this method becomes nearly impossible.)

Some daring souls have been known to use fake ID and cards to subscribe to a cellular service, then burn out the phone before the first month's bill arrives to the unsuspecting real person.

Conclusion

The future for cellular fraud is wide open. As the secret software of the over 300 brands of cellular phones in existence becomes "cracked" and re-written and spread via the underground, fraud will increase like wildfire. Virtually nothing can be done to stop the informed phone phreak as he will change ESN/MIN's, etc. easily and frequently. A new era not seen since the 2900 hertz tone was discovered is just now dawning via cellular phreaking.

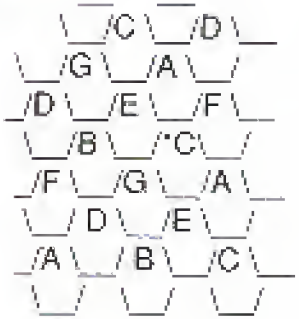
Since I'm letting the cat out of the bag for the first time here, I hereby dub the box needed to read reverse channels the BOO Box! (Shit, after 12 years I finally got to name a box.)

Cellular Magic

(continued from page 11)

825.990	825.540	825.690	825.540	825.630	825.540	825.090
825.180	825.030	825.480	825.630	825.480	825.480	825.030
825.330	825.180	825.030	825.180	825.330	825.330	825.180
825.480	825.030	825.030	825.030	825.030	825.030	825.180
825.630	825.330	825.630	825.630	825.630	825.630	825.630
825.480	825.330	825.630	825.630	825.630	825.630	825.630
825.330	825.330	825.630	825.630	825.630	825.630	825.630
825.180	825.180	825.030	825.030	825.030	825.030	825.030
825.030	825.030	825.480	825.480	825.480	825.030	825.030
825.180	825.180	825.630	825.630	825.630	825.630	825.480
825.480	825.180	825.630	825.630	825.630	825.630	825.630
825.330	825.330	825.630	825.630	825.630	825.630	825.630
825.330	825.330	825.630	825.630	825.630	825.630	825.630

Monitoring of the base sites is obviously going to be easier than monitoring the mobiles. The cell base sites are towers (usually blue) with a triangle shaped "head" on top, and sporting a couple of what appear to be vertical antennae. These base sites have a range of three to five miles. If you take a look at the honeycomb diagram, you can see how they are laid out. The cell transmitter is in the middle of the cell. It is possible to hear many, most, or all of the cells in your city, depending on your location. The closer you live to a boundary, the greater the chances of you being able to receive more cells. Due to the nature of radio signals, the actual cell shape is more or less round. However, the hexagon shape lends itself better to show how the system is laid out. With a circular coverage area, there will be some overlapping between adjacent cells.



If, for example, you live near the asterisk (*) in the above diagram, you will be able to easily hear the G, C, E, and A cells you're near. Since the maximum *practical* range of a cell is three to five miles, you'll be able to hear those a bit further away. However, due to the nature of the FM transceivers at the cell sites (they capture only the strongest signal), you should be able to hear all seven cells. Which one of each cell you hear will depend on your location and the strength of the received signal. In the above diagram, you'll most likely hear the F cell in the upper right, rather than the one on the left.

Mobile reception is almost a waste of time unless you have an outdoor antenna. And, since the mobile will be receiving on the cell site, it's better to listen to the cell frequencies. You may not be able to hear both sides of the conversation if you listen only to the mobile frequencies" but is useful, however, for determining which channel cell you're in. If you use the antenna that came with the scanner, mobile range will be decreased down to one or two miles. By choosing the scanner readout (again the cell list shown 1993.830-846.990 MHz), you can tell what cell the mobile is in. This is also useful on the cell site frequencies. If you hear someone say, "I'm at the corner of highway FF and 32," and you know where the cell site antenna is in that area, you can check the frequency listing above and determine what cell that antenna belongs to.

Where to Get What You Need!

Obviously, a device is needed to download all those ESN/MIN, etc. off the cellular airwaves. Here's the stuff I found so far one is under $2000 this ain't a cheap hobby).

CCS Company, P.O. Box 11191, Milwaukee, WI 53211 (414-781-2442) They sell everything you need for $300 to $400. Kits are cheaper. Their device interfaces between an 800 mhz capable scanner and your computer. Make sure you tell them you want the REVERSE model DIE (This is wise here.)

Curtis Electro Devices, 1235 Pear Ave. Mountain View, CA 94043 (800-332-2790, Fax 415-964-3574) They sell an ESN reader for $1295 that can read ESN/MIN, etc. but only from a short distance (maximum is 30 feet). They also sell a security model for $1595 and a NAM programmer for $1195. They publish a book called NAMFAX for $179 that tells you how to re-program hundreds of different cellulars through the keypad on the handset. (Note: You can't reprogram ESN's through the keypad unless you re-write the phone's software.)

Wavetek Communications Div., 5808 Churchman Bypass, Indianapolis, IN 46203-6109 (800-345-6356 or 317-788-5965) They sell a "Cellular I.D. Tester" that's real similar to Curtis's ESN reader but supposedly has a longer range. Price: $1495.

Needham Electronics, 4539 Orange Grove Ave., Sacramento, CA 95841 (916-924-8037) They sell reprom burners for $139.95 (I bought one myself).

Motorola (800-433-5202) They sell a cellular service manual that's used in their cellular service classes for $30. Ask for the Order Fulfillment department. Item # 68-P81150B40. This manual tells it all! An absolute must to have.

Bishop Company (800-829-0572) They publish books similar to Curtis's Samtec. Send for catalog.

Cellular Security

Well, we know a properly cloned cell phone is virtually impossible to detect. Or is it? Security companies rely on matching call patterns of subscribers' histories to current use. I.e., when 200 calls to Egypt show up in a day or 40 long distance calls to Calman, Alabama show up in a short period, all kinds of flags and whistles go off! The security companies will even keep records of people that call numbers that have been previously called by fraudulent phones and flag the phone calling that number as a potential fraudulent phone. These flags can be set to go off by a number of parameters: number of long distance calls per hour/day/month, etc. Another method they use is when the real phone places a call and the fraudulent phone places another call soon afterwards, but from a distance from the first call that's impossible to travel in such a short period of time. Example: At 5 pm Friday Phone A calls from Manhattan and completes call at 5:05 pm. At 5:12 pm Cloned Phone B calls from Queens. No one can travel those distances in two minutes, thus that ESN/MIN is flagged as a clone by the phone company. These databases are just now starting to be used in larger cities. Some software will track a rigged cell phone from cell site to cell site.

Counter-disappointers cell company software looks for an different ESN's manufacturer, model, SCM's, etc. that are broadcast by the cellular phone on its REVERSE channel. (If one captures all that data off the reverse channel and incorporates it in the cloned phone, detection via this method becomes nearly impossible.)

Some daring souls have been known to use fake ID and cards to subscribe to a cellular service, then run out the phone before the first month's bill arrives to the unsuspecting cell person.

Conclusion

The future for cellular fraud is wide open. As the secret software of the over 300 brands of cellular phones in existence becomes "cracked" and new ways and spread via the underground, fraud will increase like wildfire. Virtually nothing can be done to stop the informed phone phreak as he will change ESN/MIN's, etc. easily and frequently. A new era not seen since the 2600 hertz tone was discovered is just now dawning via cellular preacking.

Since I'm letting the cat out of the bag for the first time here, I hereby dub the box needed to read reverse channels the 1600 Box! (Stat. after 12 years I finally get to name a box.)

acronyms a-g

by Echo

Here is a list of telco acronyms that I put together. I cannot take full credit however. I have to thank many in the hp community seeing as I got much of the list from files and bulletin boards. If anyone finds this list incomplete then please send contributions to 2600.

3ACC 3A Central Control
5XBCOSR 5 X-Bar Central Office Equipment Reports system
A/D Analog to Digital
AAX Automated Attendant eXchange
ABATS Automatic Bit Access Test System
ABHC Average Busy Hour Calls
ABS Alternative Billing Service
ABSBH Average Busy Season Busy Hour
ACE Announcement Circuit Equipment
ACU Automatic Calling Unit
ADCCP Advanced Data Communications Control Procedure
ADCI Automatic Display Call Indicator
ADN Abbreviated Dialing Number
ADS Advanced Digital System
ADS Audio Distribution System
ADS Auxiliary Data System
AFACTS Automatic FACilities Test System
AFADS Automatic Force Adjustment Data System
AFSK Automatic Frequency Shift Keying
AIC Automatic Intercept Center
AICC Automatic Intercept Communications Controller
AIOD Automatic Identification Outward Dialing
AIS Automatic Intercept System
ALBO Automatic Line BuildOut
ALFE Analog Line Front End
ALGOL ALGOrithmic computer Language
ALI Automatic Location Identification
ALIT Automatic Line Insulation Testing
ALRU Automatic Line Record Update
ALS Automated List Service
AM Administrative Module
AM Amplitude Modulation
AMA Automatic Message Accounting
AMACS AMA Collection System
AMARC AMA Recording Center
AMASE AMA Standard Entry
AMAT AMA Transmitter
AMATPS AMA TeleProcessing System
AMERITECH AMERican Information TECHnologies
AMPS Advanced Mobile Phone Service
AN Associated Number
ANA Automatic Number Announcement
ANC All Number Calling
ANI Automatic Number Identification
ANIF Automatic Number Identification Failure
ANSI American National Standards Institute
ACSS Auxiliary Operator Service System
AP Attached Processor
APC AMARC Protocol Converter
APS Automatic Protection Switch
AR Alarm Report
ARC Audio Response Controller
ARIS Automated Recorded Information System
ARS Alternate Route Selection
ARSB Automated Repair Service Bureau
ARU Audio Response Unit
ASCII American Standard Code for Information Interchange
ASCC Administrative Services Oversight Center
ASPEN Automatic System for Performance Evaluation of the Network
AT Access Tandem
AT&T American Telephone and Telegraph
ATB All Trunks Busy
ATC Automatic Transmission Control
ATH Abbreviated Trouble History
ATI Automatic Testing Unit
ATIS Automatic Transmitter Identification System
ATM Automatic Teller Machine
ATMS Automated Trunk Measurement System
ATP All Tests Pass
ATR Alternate Trunk Routing
ATRS Automatic Trouble Reporting System
ATTC Automatic Transmission Testing Control center
ATTCOM AT&T COMmunications
ATTIS AT&T Information System
AUDIX AUDio Information eXchange
AUTODIN AUTOmatic Digital Network
AUTOSECOM AUTOmatic SECure Voice COMmunications
AUTOVON AUTOmatic VOice Network
AUXF AUXiliary Frame
AVD Alternate Voice Data
B6ZS Bipolar with 6 Zero Substitution
B911 Basic 911
BANAF BELLCORE AMA Format
BANCS Bell Administrative Network Communications System
BAPCO BellSouth Advertising & Publishing COmpany
BCC Blocked Call Cleared
BCD Binary Coded Decimal
BCD Blocked Call Delayed
BCS Batch Change Supplement
BDT Billing Data Transmitter
BEF Band Elimination Filter
BELLCORE BELl COmmunications REsearch
BER Bit Error Rate
BERT Bit Error Rate Test
BETRS Basic Exchange Telecommunications Radio Service
BHC Busy Hour Calls
BISP Business Information System Program
BITNET Because It's Time NETwork
BLIDS Busy Line Dont Answer
BLF Busy Line Field
BLS Business Listing Service
BLV Busy Line Verification
BNR Bell Northern Research Corporation
BNS Billed Number Screening
BOC Bell Operating Company
BOR Basic Output Report
BORSCHT Battery, Overvoltage, Ringing, Supervision, Coding, Hybrid, Testing
BOS Business Office Supervisor
BOSS Billing and Order Support System
BOT Beginning Of Tape
BPI Bits Per Inch
BPOC Bell Point Of Contact
BPS Bits Per Second
BPSS Basic Packet Switching Service

BRAT Business Residence Account Tracking System
BRCS Business Residence Custom Service
BRI Basic Rate Interface
BRM Base Remote Module
BS Bandoc Signaling
BSA Basic Serving Arrangements
BSBH Busy Season Busy Hour
BSC Business Service Center
BSCM Synchronous Communications Module
BSE Basic Service Elements
BSF Bell Shock Force
BSOC Bell Systems Operating Company
BSP Bell System Practice
BSRFS Bell System Reference Frequency Standard
BST Basic Services Terminal
BSTJ Bell System Technical Journal
BT Bus Terminator
BTAM Basic Telecommunications Access Message
BTL Bell Telephone Laboratories
BTN Billing Telephone Number
BTU British Thermal Unit
BVA Billing Validation Application
BVC Billing Validation Center
BWM Broadcast Warning Message
BWT Broadcast Warning TWX
BWTS BandWidth Test Set
C6 CABS
CABS Carrier Access Billing System
CAC Calling card Authorization Center
CAC Carrier Access Code
CAC Circuit Administration Center
CAC Customer Administration Center
CAD Computer-Aided Dispatch
CADV Combined Alternate Data/Voice
CAI Call Assembly Index
CAIS Collocated Automatic Intercept System
CALRS Centralized Automatic Loop Reporting System
CAMA Centralized Automatic Message Accounting
CAMOT Centralized Automatic Reporting On Trunks
CAS Circuit Associated Signaling
CAS Computerized Autodial System
CAT Craft Access Terminal
CATLAS Centralized Automatic Trouble Locating and Analysis System
CBS CrossBar Switching
CBX Computerized Branch eXchange
CC Central Control
CC Common Control
CC Country Code
CCC Central Control Complex
CCC Computer Control Center
CCH Connections per Circuit per Hour
CCIR Comite Consultatif International des Radio Communications
CCIS Common Channel Interoffice Signaling
CCITT Comite Consultatif International Telegraphique et Telephonique
CCNC Common Channel Network Controller
CCNC Computer/Communications Network Center
CCR Customer-Controlled Reconfiguration
CCS Common Channel Signaling
CCS Hundred (C) Call Seconds
CCSA Common-Control Switching Arrangement
CCT Central Control Terminal
CCTAC Computer Communications Trouble Analysis Center
CCU CCIT Computer Unit
CCV Calling Card Validation
CDA Dial Data Accumulator
CDA Coin Detection and Announcement
CDAR Customer Dialed Account Recording
CDCI Centralized Disconnect Cash Flow
CDF Combined Distributing Frame
CDI Circle Digit Identification
CDO Community Dial Office
CDPR Customer Dial Pulse Receiver
CDR Call Detail Recording
CDS Craft Dispatch System
CEF Cable Entrance Facility
CEI Comparably Efficient Interconnection
CEV Controlled Environment Vault
CF Call Fire
CFCA Communications Fraud Control Association
CFR Code of Federal Regulations
CGN Communication Group Number
CIC Carrier Identification Code
CICS Customer Information Control System
CII Call Identity Index
CIS Customized Intercept Service
CLASS Centralized Local Area Selective Signaling
CLASS Custom Local Area Signaling Service
CLIDN Calling Line Directory Number
CLEI Common Language Equipment Identification
CLI Calling Line Ident
CLID Calling Line Identification
CLLI Common Language Location Identification
CMAC Centralized Maintenance and Administration Center
CMC Construction Maintenance Center
CMDF Combined Main Distributing Frame
CMDS Centralized Message Data System
CMS Call Management System
CMS Circuit Maintenance System
CMS Communications Management Subsystem
CMS Communications Monitoring System
CMT Cellular Mobile Telephone
CMU CCLT Measurement Unit
CN Change Notice
CNA Customer Name/Address
CNA Communications Network Application
CNAB Customer Name/Address Bureau
CNCC Customer Network Control Center
CNI Common Network Interface
CNMS Cylink Network Management System
CNS Complementary Network Service
CO Central Office
COAM Customer Owned And Maintained
COC Central Order Control
COCOT Customer Owned Coin-Operated Telephone
CODCI Central Office Data Connecting Facility
CODEC COder DECoder
COE Central Office Equipment
COEES COE Engineering System
COLT Central Office Line Tester
COMSAT COMmunications SATellite
CONN CONNector
CONTAC Central Office NeTwork Access
CONUS CONtinental United States
CORNET COrporate NETwork
COSMIC COmmon Systems Main InterConnection frame system
COSMOS COmputerized System for Mainframe OperationS
COT Central Office Terminal
CP Control Program
CPC Cellular Phone Company
CPC Circuit Provisioning Center
CPU Central Pulse Distributor
CPE Customer Premises Equipment
CPH Cost Per Hour

CPI Computer Private Branch exchange Interface
CPM Cost Per Minute
CPMP Carrier Performance Measurement Plan
CPU Central Processing Unit
CRAS Cable Repair Administrative System
CRC Customer Service Center
CRC Cyclic Redundancy Check
CRIS Converged Range Extension with Calls
CRPMP Cable Repair Force Management Plan
CRIS Customer Record Information System
CRS Centralized Results System
CRSAB Centralized Repair Service Answering Bureau
CRT Cathode Ray Tube
CSA Carrier Serving Area
CSACC Customer Service Administration Control Center
CSAIL Centralized System for Analysis Reporting
CSC Cell Site Controller
CSDC Circuit Switched Digital Capability
CSNET Computer Science NETwork
CSO Central Services Organization
CSS Computer Side-System
CSU Channel Service Unit
CTC Central Test Center
CTM Central Trunk Module
CTMS Carrier Transmission Measuring System
CTO Call Transfer Override
CTSS Cray Time Sharing System
CTT Cartridge Tape Transport
CTTC Cartridge Tape Transport Controller
CTTN Cable Trunk Ticket Number
CU Control Unit
CU Customer Unit
CUTK Customer Update/Quick-Add system
CWCRIT Capital Utilization Criteria
CVR Compressed Voice Response
CWC City Wide Centrex
D/A Digital to Analog
DA Directory Assistance
DACS Digital Access Cross-connect System
DACS Directory Assistance Charging System
DARS Distributed Automatic Intercept System
DARC Division Alarm Recording Center
DARU Distributed automatic intercept system Audio Response Unit
DAS Directory Assistance System
DAS Distribution Area Scanner
DAS WDT Distribution Area Scanner Watch Dog Timer
DASD Direct Access Storage Device
DAV Data Above Voice
DB Decibel
DBA Data Base Administrator
DBAC Data Base Administration Center
DBAS Data Base Administration System
DBM DataBase Manager
DBS Duplex Bus Selector
DCCS DiCom Communications Shared Segment
DCE Data Circuit-terminating Equipment
DCH D Channel Handler
DCL DCC Control Language
DCLU Digital Carrier Line Unit
DCM Digital Carrier Module
DCMS Distributed Call Measurement System
DCMU Digital Conversation Measurement Unit
DCP Duplex Central Processor
DCPF Detailed Continuity Property Record (PIC)/OCPF)
DCPSK Differential Coherent Phase-Shift Keying
DCS Digital Cross-connect System
DCT Digital Carrier Trunk
DCTN Defense Commercial Telecommunications Network
DCTS Dimension Custom Telephone Service
DDC Direct Department Calling
DDD Direct Distance Dialing
DDN Defense Data Network
DDS Digital Data Service
DDS Digital data System
DDS Digital Subscriber Service
DDX Distributed Data eXchange
DEC Digital Equipment Corporation
DEFP Defective Equipment Replacement Program
DES Data Encryption Standard
DEW Distant Early Warning (line)
DFI Digital Facility Interface
DFMS Digital Facility Management System
DIC Digital Interface Controller
DID Direct Inward Dialing
DIF Digital Interface Frame
DIM Data In the Middle
DIP Dual In-line Package
DISA Direct Inward System Access
DIU Digital Interface Unit
DLC Digital Loop Carrier
DLCU Digital Line Carrier Unit
DLL Dial Long Lines
DLS Digital Link Service
DLTU Digital Line/Trunk Unit
DLU FG Digital Line Unit Pair Gain
DM Data Modulator
DMA Direct Memory Access
DMI Digital Multiplexed Interface
DML Data Manipulation Logic
DMS Data Management System
DMS Digital Multiplexed System
DMU Data Manipulation Unit
DN Directory Number
DNC Dynamic Network Controller
DNHR Dynamic Non-Hierarchical Routing
DNIC Data Network Identification Code
DNR Dialed Number Recorder
DNX Dynamic Network Xconnect
DOC Domestic Overload Control
DOCS Display Operator Console System
DOJ Department Of Justice
DOW Dots On Master group
DOTS Digital Office Timing Supply
DOV Data Over Voice
DP Demarcation Point
DP Dial Pulse
DPAC Dedicated Plant Assignment Center
DPC Destination Point Code
DPE Data Path Extender
DPN PH Data Packet Network Packet Handler
DPP Decoupled Payback Period
DPSK Differential Phased Shift Keying
DR Data Ready
DR Data Receive
DRMU Digital Remote Measurement Unit
DS Digital carrier Scan
DS Digital Signal
DS Direct Signal
DSBAV Double-SideBand Amplitude Module
DSC Direct Service Dial Capability
DSI Digital Speech Interpolation
DSN Digital Signal level N
DSP Digital Signal Processor
DSR Dynamic Service Register
DSS Data Station Selector
DSU Data Service Unit
DSX Digital System Xconnect
DT Data Terminal
DT Digroup Terminal
DTAS Digital Test Access System
DTC Digroup Terminal Controller
DTC Digital Trunk Controller
DTE Data Terminal Equipment
DTF Dial Tone First
DTG Direct Trunk Group
DTIF Digital Transmission Interface Frame
DTMF Dual Tone Multi Frequency
DTU Digroup Terminal Unit
DUV Data Under Voice
DVX Digital Voice eXchange
E&M (Ear & Mouth) or (Earth & Magneto) & Mouth signaling
E-COM Electronic Computer Originated Mail
E911 Enhanced 911
EADAS Engineering and Administrative Data Acquisition System
EADAS/NM EADAS/Network Management
EAEO Equal Access End Office
EARN European Academic Research Network
EAS Extended Area Conductor Unit System
EAS Extended Area Service
EASD Equal Access Service Date
EBCDIC Extended Binary Coded Decimal Interexchange Code
ECAP Electronic Customer Access Program
ECC Error Check Character
ECCS Economic Calculated Call Seconds
ECF Enhanced Connectivity Facility
ECPT Electronic Coin Public Telephone
ECS Electronic Crossconnect System
EDAC Error-correcting Digital Adapter Circuit
EDI Electronic Data Interchange
EDP Electronic Data Processing
EDSX Electronic Digital Signal Xconnect
EECT End to End Call Trace
EEDP Expanded Electronic Tandem Switching Dialing Plan
EEHO Either End Hog Off
EEI Equipment-to-Equipment Interface
EERAP Electronic Feeder Route Analysis Program
EIA Electronics Industries Association
EIS Expanded Inband Signaling
EISS Economic Impact Study System
EKTS Electronic Key Telephone Sets
EML Expected Measures Loss
EMS Expanded Memory Specification
EAFM Exchange Network Facility for Interstate Access
EO End Office
EOE Electronic Order Exchange
EOS Extended Operating System
EOTT End Office Toll Trunking
EPL Electronic switching system Program Language
EPROM Erasable Programmable Read-Only Memory
EPSCS Enhanced Private Switched Communications Service
ER Error Register
ERAR Error Return Address Register
ERER Environmental Recording Editing and Printing
ERL Echo Return Loss
ERP Effective Radiated Power
ERU Error Return address Update
ESAC Electronic Surveillance Assistance Center
ESB Emergency Service Bureau
ESF Extended SuperFrame
ESL Emergency Stand Alone
ESN Electronic Serial Number
ESN Electronic Switched Network
ESP Enhanced Service Provider
ESS Electronic Switching System
ESSX Electronic Switching System eXchange
ETAS Emergency Technical Assistance
ETF Electronic Toll Fraud
ETN Electronic Tandem Network
ETS Electronic Tandem Switching
ETS Electronic Translation System
ETSACI Electronic Tandem Switching Administrative Channel Interface
ETSSP ETS Status Panel
FA Fuse Alarm
FACS Facilities Assignment and Control System
FAR Federal Acquisition Regulation
FAST Fast Application System Test
FAT File Allocation Table
FCAP Facility CAPacity
FCC Federal Communications Commission
FCC Forward Command Channel
FCG False Current to Ground
FCS File Control Systemaction
FCS Frame Check Sequence
FDM Frequency-Division Multiplexing
FDP Field Development Program
FDX Full Duplex
FED Far End Data
FEMF Foreign Electro Motive Force
FEPS Facility and Equipment Planning System
FEV Far End Voice
FGA Feature Group A
FGB Feature Group B
FGC Feature Group C
FGD Feature Group D
FIFO First In, First Out
FIOC Frame Input/Output Controller
FIP Facility Interface Processor
FIPS Federal Information Processing Standards
FM Frequency Modulation
FMAC Facility Maintenance And Control
FNPA Foreign Numbering Plan Area
FOC Fiber Optic Communications
FON Fiber Optics Network
FR Fast Rate
FRS Flexible Route Selection
FSK Frequency Shift Keying
FTG Final Trunk Group
FTP File Transfer Protocol
FTS Federal Telecommunications System
FX Foreign eXchange
GBS Group Bridging Service
GCS Group Control System
GEISCO General Electric Information Services Company
GHZ GigaHertz
GID Group ID
GND Ground
GOC Global Outside
GOS Grade Of Service
GP Group Processor
GPIB General Purpose Interface Bus
GRD GRounD
GRP MOD GROUP MODulator
GSA General Services Administration
GSAT General telephone and electronics SATellite corporation
GTC General Telephone Company
GTE General Telephone Electronics
GTT Global Title Translation

Looks like that's all we can fit for now. But the second half will be even more thrilling!

A STUDY OF HACKERS

by Dr. Williams

In *The Hacker's Handbook* on page 123, Hugh Cornwall discussed an idea of setting up his home computer system to look and act like a mainframe system. He would let hackers attempt to gain access to it while he monitored the results. He wanted his home system to emulate the MI5, the most notorious hacking target for British hackers. The hackers would get into the system and attempt to gain privileges, when unknowingly they were really trying to get into his system. Hugh did not carry out the plan, even though he did set up a sophisticated simulation of the MI5. About the time he was to carry out his plan, a disgruntled employee left the MI5 crew, and went to the News hanging out all of the dirty laundry. Hugh thought carrying out the stunt may get him into trouble, or at least more publicity than he wanted, so he didn't go through with it.

I just carried out this idea myself, and I thought the results were interesting.

I had just completed a class in operating systems. The class used MINIX as a model to study and modify. MINIX is an operating system compatible with version 7 of UNIX, specifically made to be run on IBM and its clones. It has over 12,000 lines of source code written in C. After finishing the class, I decided to use MINIX because I thought it could best mimic a big computer system under the guise of UNIX.

It took me a while to build an appropriate "pseudo-system"; one that I thought was capable of fooling novice users of UNIX into thinking they were indeed on a UNIX system. It would have been beyond the capacities of my machine to do all that was necessary to fool expert users of UNIX though, not to mention the time constraints I had. First I had to reformat my hard drive for the MINIX operating system. Then I had to write a device driver to run the modem, which took a while to do. I had to change physical appearances: names of file, directories, syntax of items, and emulation style. I added some characteristics - putting in games, files with interesting names, eye catching items, and additional mail facilities. Finally, I wrote the program which did the actual mimicking, which also gathered statistics of the users' activities. Overall, I spent six months worth of free time making a satisfactory system.

The program was made to imitate UNIX in all regards. At various times, it would 'show' different users on, different processes being run, disk quota, terminal statistics, free spaces, printer job status, and so on. It showed different disk packs, had most of the files which UNIX uses for system and administrative functions, and backup schedules.

On the login screen, I was tempted to put something like 'Boeing node #2, please login', or 'General Dynamics Site 3, spot 2'. However, I thought this could get me more trouble or attention than I wanted, so I settled for a more generic approach:

BN Site #2
«current time»
please log in:

After login the first screen would show:

There was a crash on /group3 on 6/8/89 at approximately 03:00. Some files from that location have been deleted. Please inspect your account for file integrity. Call the operators at ext. 3524 if you need to get any files from backups. There will be a gathering on 6/24/89 at noon in the cafeteria during lunch for all employees wishing to form a group of people interested in remote control cars and planes. Please call Jeff Smith at ext 2146 for further details.

And the prompt was:

June[1]

Every time a command was entered, the number in the square brackets was incremented by one.

In the program, I left in some famous UNIX bugs, hoping somebody would try to manipulate the account into getting more privileges. I left in mail bugs, writing commands to the 25th line, and using the same encryption scheme for the password file which UNIX uses, and a few other smaller items. To egg them on, I put in games which could only be executed with privileges, and files with tempting names like CAR.DATA, PRIVATE.DOC, and DOCUM.SECRT which also could only be read with privileges. Every time the account logged off, I returned most things back to the original setting, including any gains they had made. So if a person logged on more than once, they had to start from scratch every time. I didn't like doing this, but since I thought a lot of people would be using a few accounts, I thought it would look more phony if the account drastically changed every time the person logged onto it. It also helped me make more accurate observations. At this time, I got a friend to agree to give up his dorm room phone for a few months, since he was taking off anyway. So I plugged the computer into there and let 'er rip.

I wanted to put the accounts into three different targets: hackers, hacker wanna-be's, and the academic community. On the bulletin boards which I had hacker privileges on, I posted a message telling users to call this "neat" system I discovered. The message went something like:

"I recently discovered an account to a UNIX system at 555-5555.
The account name is 'PAULS', with password 'dogSpot'.
Have fun!"

A day later, I posted the same sort of message on different bulletin boards, those which I had only a normal status on, but where there were more "kiddies" on. I changed the account name and password. Finally, a week later, I told some of my friends by word of mouth in the academic community, but with another different account/password combination.

Something that I predicted would happen is that a lot of the sysops whose system I had posted the message aimed for the "kiddies" erased the message. Over half of them had erased the message in less than a few hours. The other half had the message erased in about a day. It still served my purpose though, because a lot of people had seen the message. I was tempted to tell the sysops whose system I had posted the message on that it was all a hoax - an experiment, but I thought some of them wouldn't keep the lid on that information.

Something which I sort of expected was that a lot of the sysops wrote me mail back, furious that I had posted that message. Most of them thought I was putting them in legal jeopardy (understandably). Others said that their board was not into that type of information, threatened to call the police, warned me to never post that type of message again, and even deleted my account (no loss). None of the messages to the hacker crowd were lost. I posted the message 17 times for the kiddies, five times for the hackers, and told four friends who I know passed it on to a few other people.

I suppose if somebody would have thought about it, he or she might have concluded that it's pretty hokey to post an account/password combination on a public BBS room where everybody can read it. Either I had to be really arrogant, or have ulterior motives.

Within eight hours of posting the message, the system got its first call. I was really hoping that it would be somebody who knew what they were doing. I wanted to see if anyone was going to be able to jump the hoops I set up to gain further privileges. The first person didn't seem to be familiar with the UNIX operating system - they kept on trying MS-DOS commands. They couldn't do a disk directory, or any other basic operations in UNIX. In fairness, if you're not used to UNIX, it is pretty user unfriendly.

The next few callers seemed to know more about what was going on. They were logged on under the hackers' account. They were able to find out the attributes of the account, get a view of what the overall system looked like, and see what the range of the system was. A few of those were able to locate some of the targets of interest I put in, but did not gain access.

Next, the kiddies' account took a big jump in usage. The majority of them were unfamiliar with the UNIX system. Some of them had a cursory knowledge of the basic UNIX commands, but didn't really know how to manipulate the machine.

Finally, a few calls started coming in on the academic account. Most of them didn't spend too long on the account. Since they knew more about what was going on, they took a look to see what was around and split. One or two of them tried using some of the more sophisticated commands which work on UNIX, but not on MINIX.

Over a two month period, I was able to see what the overall attributes of usage were. I don't know how many unique individuals logged into the account, but I did keep track of how many times the account was used. By looking at the log of commands from the kiddie account, about half of its usage came from people unfamiliar with UNIX. Using MS-DOS commands or commands of other PC's, inability to access the help file, and no experience with the UNIX environment were characteristic of these users. Approximately a quarter of the usage came from people who had

exposure to UNIX with a basic knowledge. They were able to find out the basic structure of the account and system, wander around a bit, but did not do anything sophisticated. The last quarter had at least competent users: some where quite expert. They were able to discover items of interest, find most items of importance, gain further privileges, and attempt to hide the account that had been used.

From the 50 percent of users who were UNIX competent, only one third of them tried to gain privileges. The other two thirds must have been content where they were at. Of the others, the most popular scheme used to gain privileges was to read the password file (which, like in UNIX, is publicly readable but encrypted). This was not a bit surprising to me, since the Cornell Worm used essentially the same method. Many articles have talked about it, some showing how in a cookbook recipe manner the steps were taken. Users would try to decrypt the password file and gain the root password. The next most common method was written commands to the 25th line of a more privileged account. This wasn't surprising either, since much ado has been made about that. The rest seemed to be evenly spread around on real bugs, finding bugs in commands which run shells in privileged modes, or some other method.

From the third of the users left over, 32 percent of them succeeded in raising the account's privileges. Out of that 32 percent, 68 percent of the people were able to get at least operator privileges. Out of that 68 percent, 18 percent (25 people) were able to get root privileges. I didn't know though if that was one person who got root privileges 25 times, or 25 different people. The program I had written really only mimicked the root privilege, and did not allow total control of the machine.

The sophistication of the user was directly related to the amount of "stupid" things the user did. Some of the kiddies did some real stupid things, like creating files saying something like, "Ha. Ha. I'm a hacker and I'm in your system.", deleting files, or editing files in an obvious manner. Others romped around the system, checking out every file in every sub directory. Other items which were not as obvious were using the help files excessively, entering many incorrect commands consecutively, and continually trying to access items for which they had insufficient privileges. The most knowledgeable users tried to hide their presence. Some of them successfully edited the user log without leaving a trace, kept a low profile of activities, and did not play the games at all or for great lengths of time. Out of those who gained privileges, there was only one incidence of someone deleting a file on purpose without cause.

Overall, the kiddie account logged in 2,037 users. The hacker account logged 1,432 users, and the academic account logged 385 users. I have no way of knowing though how many unique people used the accounts. I was disappointed at the low turnout from the academic community. I talked to somebody I had given the account to, and some of the reasons seemed to be that some people just weren't into hacking, had legitimate accounts, were not curious about other systems, and just didn't want to risk getting into trouble.

Overall, the most incompetent users came from the kiddie account. The hacker account seemed to be most familiar with all of the system weaknesses, but lacked an overall understanding of the system. The academic account was just the opposite; they knew how to work the system, but did not know of the security shortcomings of UNIX. However, the best users came from the academic account, where there was probably an elite crust of students who are also hackers.

One side effect came shortly after I posted the original message on BBS's. Soon, other people started posting the kiddie account/password combo, claiming they got it from a friend or had "hacked" it themselves. That's why when the sysops deleted my message, I wasn't worried, because enough people had seen it to spread the word around.

I felt expected some law agency to raise an eyebrow and look into the matter. After all, I had done a pretty blunt thing. I did not get any questions about it though, nor did the person who owned the phone number. But then again, maybe somebody did, and I just didn't find out about it.

ALL LIFETIME SUBSCRIBERS TO 2600 WILL NOW RECEIVE 1984, 1985, AND 1986 BACK ISSUES. IF YOU'RE A CURRENT LIFETIME SUBSCRIBER, CONTACT US IF YOU WANT THESE BACK ISSUES.

2600 marketplace

COMPLETE 300+ PAGE *TAP* BACK ISSUE SET. NOT photo-reduced $85; *TEL* back issue set $10, cellular phone modification and conversion manual $9. Peregrine Dynamics, PO Box 709, Kent, Ohio 44240

MEET THE ESTABLISHMENT. Plan your calendar, scholarships available. The second annual international symposium on "National Security & National Competitiveness: Open Source Solutions" will take place in the Washington DC area the week of 2 November 1993. Cyberspace pilots and hackers in demand as speakers and to display good "hacks" pertinent to finding, collating, and presenting information useful to decision-makers. Hackers are a national resource - but the policy-makers and business barons (e.g. those uninformed by *Forbes*) need to understand this. Come strut your stuff, awe the uninitiated, have a good time. To discuss further, communicate with steeler@well.sf.ca.us or fax to (703) 536-1776.

LOOKING FOR OLD TELCO VANS for purposes too illicit to mention here. Contact BoB - (516) 751-2000.

WANTED: Any "good" text philes (*2600* related). Will pay money. Contact me on Private Idaho BBS (208) 336-9827.

DEAD PROGRAMMERS SOCIETY BBS (514) 699-7091. Seize the day. Canada's gateway.

CALLER ID'S $39.95 PPD. Surveillance, counter surveillance equipment. Catalog $5. Dealer wanted. EDE, PO Box 337, Buffalo, NY 14226.

STUDENT HACKER seeks any and all information, plans, magazines, books, schematics, etc. related to hacking, phreaking, electronics, computers, phones, cable TV. Willing to exchange any information I find from my own research. Also looking for any single issue of *TAP* and *Wired* Magazine. Write: J.C.D., 5015 Club View Drive, Concord, NC 28025.

SCANNER FOR SALE: Bearcat 800XLT (includes cellular). Excellent condition. Original box/papers, 20 hours on time. $185 insured UPS to your door. $35 for 800 MHz/cellular ground-plane antenna. Call/leave message for Jon (213) 344-9156.

THE PERFECT PORTABLE HACKING COMPUTER! NEC Ultralite Notebook Computer, 640k RAM, BACKLIT LCD. It also has a Solic State 1 Mb Silicon Disk. ALL THIS ONLY WEIGHS 4.4 LBS! Factory Refurb. Only $500!! Free built-in 2400 baud modem. For a 2mb Silicon disk add $50. For an external Disk Drive, add $50. Supplies LIMITED! Send Check or M.O + $7.50 S/H. C.O.D avail, add $4.00. AI Technologies, Inc., P.O. Box 1053, Poughkeepsie, NY 12602-1053.

THE GOLDEN ERA REBORN! Relive the thrill of the golden era of hacking through our exclusive collection of H/P BBS Message Bases. Posts from over 40 of the most popular boards such as 8BBS, OSUNY, PLOVERNET, LOD, PHOENIX PROJECT, and more. Available in IBM, Amiga, & Macintosh formats. Send for the listing by: Email: lodcom@mindvox.phantom.com. Snail Mail: LOD Communications, 635 W. 13th St., Suite 1A-278, Austin, TX 78701. Voice Mail: 512-448-8298.

IMPRISONED UNDERGROUND ENTHUSIAST seeking correspondent. Also seeking hardcopy: cyber-related publications and Usenet feeds. Please write Shrike c/o 7881 Crossfox, Boise, ID 83709.

AMIGA 2000, digitizer, RAM expander/HD controller, midi, modem, extra floppy, software. $2000/best offer. (413) 528-7827.

THIS MACHINE IS BROKEN stickers. Fluorescent red, made to last. For all of the broken machines in your life. $5 per hundred. 2600 Stickers, PO Box 752, Middle Island, NY 11953.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $1 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Summer issue: 5/15/93.

Getting your file...

by Bayonet

There exists, somewhere, a file on you. Maybe you know about it, maybe you don't. It's there either way. As some Greek guy once said, Know Thyself. At the very least, know what they know.

The following addresses are useful for getting your credit records. Call or write, and they'll probably be "kind" enough to walk you through the process of getting one. For a fee.

Equifax Credit Information Services
Box 740241
Atlanta, GA 30374-0421.
800-685-1111

Your credit history is available for $8 in Maine and Montana, $5 in Maryland, $10 in Massachusetts, free in Vermont, $8 in all other states.

TRW Consumer Complimentary Report
Box 2350
Chatsworth, CA 91313-2350
214-235-1200 (Dallas HQ)

(This is the address to use if you have not been denied credit in the past sixty days.)

Your credit history is available for free, one copy a year.

TRW Consumer Assistance Center
Box 749029
Dallas, TX 75374
214-235-1200

(This is the address to use if you have been denied credit in the past sixty days.)

Also free, also only one copy a year.

Trans Union Corp.
Box 7000
North Olmsted, OH 44070
216-779-2378

Free if you've been denied credit in the past sixty days. Otherwise, $15 for an individual account record, $30 for a joint account record.

Keep in mind. requesting copies of your credit history affects your credit history negatively! I guess they figure if a lot of people are checking you out, there must be some cause for concern. If you do this at all, do it once a year. Also a keen way to blow someone's credit rating, though the volume at which you'd have to do it would become ridiculous.

The next address is for medical information. Unlike requesting credit reports, this shouldn't adversely affect your rating.

Medical Information Bureau
Box 105
Essex Station
Boston, MA 02112
617-426-3660

Free, believe it or not.

Now for the fun stuff. Use these next addresses to get information about your criminal record, or just to see if the feds have you listed as someone worth watching. Incidentally, *if you don't have a record with them*, requesting copies of one will make them *start* one. Again, I guess the reasoning is if you ask, you must have something to hide.

Federal Bureau of Investigation
Attn: Freedom of Information Section
10th St. and Pennsylvania Ave., NW
Washington, DC 20535
202-324-5520

This is the address to use if you do not have a criminal record.

The first 100 pages are free, but then it's $0.10 a page. If your report is more than 100 pages long, well... Sully for you.

Federal Bureau of Investigation
Identification Div., Rm. 10304
10th St. and Pennsylvania Ave., NW
Washington, DC 20535
202-324-2222

This is the address to use if you do have a criminal record:

This costs you seventeen bucks, because crime (after all) doesn't pay. Criminals do.

The least interesting, but by no means least useful, address is the next one, for Social Security information.

Social Security Administration
Wilkes-Barre Data Operations Ctr.
Box 20
Wilkes-Barre, PA 18767-0020
800-772-1213

This is free. Since it's also a government office, I'd request a report three or four times a day. Get the most bang for your taxpayer buck, but please... recycle all that paper.

Lawsuit Filed Against Secret Service

Action is Taken on Behalf of DC 2600 Meeting

The Secret Service may have thought that harassing a motley crew of hackers in a shopping mall would have resulted in nothing more than the intended goal of sending them scurrying back to their underground hideouts, fearfully awaiting a knock at the door. But when the Washington D.C. *2600* meeting was detained, searched, and ejected from Pentagon City mall by mall security officials, seemingly acting on behalf of the Secret Service, we knew exactly where to go: to the press and the lawyers.

Since the incident, articles have appeared in the trade journal *Communications Daily*, the Washington *City Paper*, even a front-page story in the Washington *Post*. This is in addition to an uncountable number of pieces throughout the Internet and over bulletin boards. This was certainly more attention for anyone at the Secret Service could have anticipated.

Unfortunately for them, they were not even allowed to slink away, red-faced at their botched job. Computer Professionals for Social Responsibility, whose membership applications were seized at the November meeting, were the first to express interest in our predicament. The Electronic Frontier Foundation and the American Civil Liberties Union would soon follow in offering their legal counsel.

CPSR filed two Freedom of Information Act requests with the Secret Service on behalf of several meeting-goers who were interested in possible legal actions against the perpetrators of the "raid". The Secret Service returned the requests, saying that they had no information on any of the meeting-goers. This immediately raised suspicion, as the mall security personnel collected everyone's name and phone number at the November meeting. Presumably this information was on file somewhere. Also, one of the meeting-goers had been visited by the Secret Service about two years ago, completely unrelated to anything computer-oriented. Presumably a file was created on him at that time, and yet the Secret Service said they had no information on anyone involved. Thirdly, one of the meeting goers was visited by the Secret Service subsequent to the meeting. During this visit, one of the agents made reference to his name being on "the mail list". It seems highly unlikely that the Secret Service had absolutely no information on any of the people on whose behalf CPSR filed FOIA requests.

Acting on these strong suspicions, on February 4th, CPSR filed suit against the Secret Service for failing to provide information requested under the Freedom of Information Act. The SS has thirty days to respond.

All of this is merely a preliminary game of legal hide-and-seek to establish what role, if any, the Secret Service and other government agencies might have played in the November *2600* raid. Once everyone involved stops contradicting each other and a clearer image forms of who was behind the harassment, we can begin to consider other possible legal avenues to send the Powers That Be a strong message about what to expect when trying to intimidate a group of hackers.

Stay tuned.

2600 ROBBED OF TOUCH TONES

All right, it isn't all that much of a story. But it is worthy of reporting for nearly ten years, we've enjoyed the use of our touch tone phones here at the *2600* offices. But several months after our central office was cut over from a crossbar to a 5ESS digital switch, we found that all of our touch tone phones no longer cut the dialtone. You see, we have steadfastly refused to pay a surcharge New York Telephone levies on anyone who uses a touch tone phone. The charge is small (under $2 a month) but it's the principle. It's a fact that there is no special equipment needed to process touch tones. Quite the contrary, it takes special equipment to ignore touch tones! It's nothing short of blackmail. Our phones still generate tones that are perfectly usable - only not for dialing. Fortunately, it wasn't hard at all to switch everything - phones, computers, fax machine - to pulse dial. It takes longer to dial and the more 9's and 0's we generate, the more we fix up New York Telephone's equipment. Their loss, not ours.

To give you an idea of the absurdity of the situation, this is what New York Telephone has to enter into their computer to stop ignoring our touch tones:

RCV:APPTEXT
FORM=1VR&CHG,TN=7513600,TTC=V,END

They want to charge us $10 to type that.

British News

by The Dark Knight

Sex, Lies, and Audiotape

The government clampdown on telephone chatlines appears to have had an unfortunate effect on innocent telephone services.

Infosale, a West Country telephone-sales business, may have to close after a judge ruled that its adult dating service was a type of chatline. As such, Infosale would have to pay 20,000 pounds towards a scheme to compensate BT customers who found their phone bills had rocketed because their children were constantly telephoning chatlines.

Anthony Chappell, proprietor of Infosale, said the 20,000 pound bill would push his company into receivership. But worse still, Chappell said the regulations on chatlines would force him to record his customers' dating conversations. Chappell said the recordings would include the most intimate details.

On hearing this there are undoubtedly hundreds of *2600* readers wincing in horror at the realisation that every time they ring an adult dating service their every word is being taped. I consider this to be an outrageous invasion of privacy, and hope that there will be a change in the law.

Keeping The Poles Apart

BT engineers are up in arms about telegraph poles. They have refused to climb non-union poles which had been fitted by private firms in London and the Midlands.

It is a protest about changes to traditional working practices. The engineers had previously replaced old poles with new ones, but left the old poles to be collected at another time. This meant that they were paid twice for visiting the same site.

A compromise scheme is now in place whereby the engineers have agreed to pilot a bold new initiative dreamed up by BT.

They will collect the old poles at the same time as the new ones are fitted!

All Down To Those Family Connections

How many of you have experienced the pleasures of contacting BT's accounts department about that phone bill you know you've paid, but BT's computer says you haven't?

Sarah Carsberg was sent a final reminder and one of those friendly letters advising you that your connection is in danger of being severed if you don't cough up. She obligingly delivered the forty pounds she owed.

Unfortunately there were a few crossed wires somewhere and Sarah was cut off anyway. She complained. Nothing unusual in that, of course. People are always complaining about BT.

What is interesting is the fevered response her complaint seems to have generated. Not only was she swiftly reconnected, but BT has launched an internal inquiry into why this cock-up occurred in the first place.

Optimistic to the end, I would like to think this is indicative of a new era of customer responsibility at BT, but I can't help feeling there were other factors in play here.

You see, Sarah Carsberg just happens to be the daughter of Sir Bryan Carsberg, who just happens to be the boss of telephone watchdog Oftel, the permanent thorn in the side of BT's prancing piper.

BT Charges Frustrate Competitors

The government has received proposals from over 20 companies wanting licences to run telecommunications services, but a large number are expected to pull out because of restrictive interconnection charges.

Following market deregulation in March, the department of Trade and Industry has received bids from companies keen to compete with BT and Mercury. But the proposed new system of connection to BT's network is seen as anti-competitive.

Vivienne Peters, chief executive of the Telecommunications Users' Association, said since the access connection proposals were announced members had expressed pessimism over the likelihood of any real competition.

"The proposals are a barrier to competition as profit levels will be too narrow for reinvestment. As companies are still unsure of what the costs will be it is difficult to make business plans. I expect a huge fall off in interest," said Peters.

Recently John Redwood, corporate affairs minister at the DTI, said a number of the twenty proposals included "substantial telecommunications systems and innovative technological approaches."

National Transcommunications, the engineering arm of the former Independent Broadcasting Authority, has expressed interest in providing telecom services.

A spokesman for National Transcommunications said the company was considering a number of options that combined its traditional broadcasting skills with telecommunications.

+++

Northern Telecom has won a 5.8 million pound contract from BT's internal networks organisation. Northern Telecom is supplying an automatic call distribution system to speed up BT's pick-up rate on customer enquiries in Greater London.

+++

Dowty Communications, in collaboration with local supplier Omnicron Praha, has won orders in Czechoslovakia totalling 700,000 pounds. Dowty is to provide business and technical support as well as hardware, including X.25 packet switching networks, to the Czechoslovak state and commercial banks.

2600 MEETINGS

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: 212-223-9011,8927; 212-308-8044,8162.

Poughkeepsie

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

Washington DC

Pentagon City Mall in the food court.

Cambridge, MA

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: 203-748-9995, 203-794-9854.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: 215-222-9880, 9881, 9779, 9799, 9532; 215-387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court.

Fort Lauderdale

West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-585-9214, 100#.

Atlanta

Meetings announced on local BBS (404) 612-0340.

Chicago

Century Mall, 2828 Clark St., lower level, by the payphones: 312-929-2695, 2875, 2885, 2994, 5257.

Ann Arbor, MI

Galleria on South University. Payphones: 313-663-9727, 9410.

Bloomington, MN

Mall of America, food court.

St. Louis

Galleria. Highway 40 and Brentwood, lower level, food court area, by the theaters.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World. Payphones: 512-453-9834, 9885, 9316.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: 213-972-9858, 9886, 9506, 9519, 9520; 213-625-9923,9924; 213-614-3849, 9972, 9918,9925.

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9903,4,5,6.

Seattle

Washington State Convention Center, first floor. Payphones: 206-345-9800, 9801, 9804, 9809.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-855, +49-89-555-541, 542, 543, 544, 545.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

WHY SUBSCRIBE?

SOME OF YOU WHO PICK US UP ON NEWSSTANDS HAVE BEEN CALLING TO TELL US THAT IT'S CHEAPER TO BUY 2600 ON THE STANDS THAN IT IS TO SUBSCRIBE! WE KNOW MANY MAGAZINES OFFER NEWSSTAND DISCOUNTS. DRUG DEALERS ALSO OFFER THEIR PRODUCTS AT LOWER PRICES UNTIL YOU GET HOOKED. BUT THAT'S A BAD ANALOGY. SO WHY SUBSCRIBE? YOU WON'T HAVE TO ENGAGE IN DEGRADING STREET BRAWLS OVER THE LAST ISSUE IN YOUR LOCAL BOOKSTORE. YOU WON'T HAVE TO TOSS AND TURN AT NIGHT WONDERING IF THE BOOKSTORE CLERK IS ACTUALLY AN INFORMANT WHO WILL TURN YOU IN FOR READING SUBVERSIVE MATERIAL. YOU WON'T FACE THE RIDICULE AND SCORN THAT COMES FROM ASKING FOR A MAGAZINE THAT NOBODY ELSE HAS HEARD OF. BY SUBSCRIBING, YOU WILL GET YOUR ISSUES DELIVERED RIGHT INTO YOUR OWN HANDS A GOOD TWO WEEKS BEFORE THEY HIT THE STANDS. NO NEED TO GO OUTSIDE AND RISK INFECTION. AND ONLY SUBSCRIBERS CAN TAKE ADVANTAGE OF THE FREE 2600 MARKETPLACE!

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (also includes 1984, 1985, 1986 back issues)

BACK ISSUES ($25 per year)

❑ 1984 ❑ 1985 ❑ 1986 ❑ 1987 ❑ 1988

❑ 1989 ❑ 1990 ❑ 1991 ❑ 1992

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(Individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED:

PLEASE WRITE YOUR NAME AND ADDRESS ON BACK